ROAD TO IMPLEMENTATION

Enterprise Risk Management for Colleges and Universities

Gallagher
Higher Education Practice
Arthur J. Gallagher Risk Management Services, Inc.

Table of Contents

Section **Page**

Preface

At Gallagher, we believe that Enterprise Risk Management provides a powerful framework allowing organizations to consider the positive and negative implications of risk at all levels. In creating a common language and unified thought process for addressing risk, ERM better positions organizations to make informed decisions on allocating resources to best support their missions.

Colleges and universities are in the risk business. Risk identification, risk avoidance, risk mitigation, and risk tolerance may not be part of the everyday lexicon at most colleges and universities, but these activities are already part of every major decision made on campus. The ERM process is about identifying risks, measuring their impact, assigning ownership of the risk, and creating a framework for reporting actions taken to mitigate risk and maximize opportunity. ERM promotes innovation and instills best practices for accountability, transparency and compliance. ERM leads, in our judgment, to better management of resources and capital.

To say the least, there are myriad documents written on ERM and no limit on the availability of “how-to” guides. So why did we choose ERM as the topic for our fourth Think Tank study?

We believe we can add value to the literature by providing colleges and universities with a road map specifically designed for them on how to efficiently and cost-effectively implement ERM. Campus administrators have told us that while they believed they were informed about the concept of ERM, they remained unclear or intimidated by the process of implementing ERM. Many thoughtful leaders expressed the opinion that the available literature was geared toward commercial enterprises and did not speak to the reality of the higher education environment. By recognizing and accepting the decentralized and entrepreneurial nature of colleges and universities, we sought to develop a guide that offers practical and sustainable steps that meet the challenges of higher education operations head-on. We believe this year’s Think Tank and this document fill a void.

Once again, we were able to draw on the expertise of thought leaders within higher education who have had first-hand experience in implementing ERM on their campuses. Some have only begun the process; others have mature programs refined over several years. The spectrum of institutions was complete, from community colleges to research universities. I thank each participant who took the time to contribute to this effort.

Sincerely,

John McLaughlin
Managing Director
Higher Education Practice
Arthur J. Gallagher Risk Management Services, Inc.

September 2009

Participants in the Think Tank Process

- Sheri Ackley
  Director, Office of Safety and Loss Prevention
  University of Wisconsin System Administration

- Allen J. Bova
  Director, Risk Management and Insurance
  Cornell University

- Richard F. Denning
  President, Shelter Island Risk Services

- Dorothy M. Gjerdrum
  Executive Director
  Public Entity & Scholastic Division
  Arthur J. Gallagher Risk Management Services, Inc.

- Ann H. Franke
  President, Wise Results LLC
  Washington, DC
  Consulting *Report Editor*

- Glenn Klinksiek
  Assistant Vice President for Risk Management and Audit
  University of Chicago

- Gary W. Langsdale
  University Risk Officer
  Pennsylvania State University

- Vincent E. Morris
  Director of Risk Management
  Wheaton College
  President, University Risk Management and Insurance Association

- Ruth Unks
  Risk Manager
  Maricopa County Community College District

- Joseph Yohe
  Associate Vice President, Office of Risk Management
  Georgetown University

Special presentations were kindly provided by

- Richard D. Legon, President, Association of Governing Boards of Universities and College

- Vincent Morris, President, University Risk Management and Insurance Association
  Director of Risk Management, Wheaton College

- Dorothy Gjerdrum, Chair, U.S. Technical Advisory Group for Risk Management,
  International Standards Organization
  Executive Director, Public Entity & Scholastic Division,
  Arthur J. Gallagher Risk Management Services, Inc.

Representatives of Arthur J. Gallagher Risk Management Services, Inc.

- John McLaughlin, Managing Director, Higher Education Practice

- Leta Finch, Executive Director, Higher Education Practice

- John E. Watson, Executive Director, Higher Education Practice

Introduction

New opportunities and challenges emerge every day for colleges and universities. In this dynamic environment, institutions face uncertainty over whether they will achieve their goals. Uncertainty derives from unpredictable internal and external factors. With uncertainty, the risks of achieving institutional goals can become intricately and hugely challenging. Enterprise Risk Management ("ERM") is a way to better manage the challenge. This report begins with a brief introduction to ERM and then provides detailed practical guidance on how an institution can implement ERM.

Risk can be defined in many ways. Nearly every practitioner, consultant, and report offers a different definition. Looking at risk broadly as the *effect of uncertainty on objectives*, it becomes clear that risk has both positive and negative aspects. An important element of ERM is appreciating that from proactive management of risk across the enterprise, one can more readily realize the benefits of risk taking and thus more assuredly achieve goals.

ERM is a cyclical process, as working toward any goal itself leads to new opportunities and challenges. Take, for example, the goal to raise $50 million for a capital campaign. The fundraising process needs to be managed as carefully as the ensuing construction process once the money has been raised. Achieving the goal created more resources. Consider, too, the consequences of losing $50 million unexpectedly. That occurrence also needs risk management to mitigate the negative impact of such a significant financial loss.

We embrace the definition of ERM as *the commitment to managing risk as an integral component of an entity's operations in order to maximize opportunities and minimize setbacks to the entity's mission, strategies, and objectives.*[1] ERM links the effects of risk to overall institutional strategy. It influences decisions made at every level. With ERM, an institution can achieve a continuous cycle of improvement throughout its operations. At its most powerful, ERM reassures the governing board that the institution uses solid procedures that advance its goals and minimize unnecessary costs, reputational damage, and other adverse consequences.

Higher education has become a dynamic and fluid environment that generates and assumes considerable risk. Factors contributing to change over the past decade include:

- *Globalization.* Students are studying abroad in greater numbers, more students are doing international experiential learning projects, and many colleges and universities have opened foreign campuses. Each of these developments creates uncertainty and touches many departments throughout the institution.

- *The economy.* Institutions are facing critical needs to increase efficiencies, capitalize on innovative research, and take other steps to meet financial challenges. Expedited decisions may be necessary to meet pressing financial challenges.

- *Competition and student demands.* Four students sharing a dorm room, once widely accepted, is now considered overcrowded. Today, few students have ever shared a bedroom at home and they don't want to do so at college. The building boom in student housing, recreational facilities, and state-of-the-art classroom space has created significant risks that have touched departments all across campus.

[1] International Standards Organization 31000 sample Risk Management Policy.

- *The threat of campus violence.* Too many examples of campus violence and death have made the unthinkable a real threat on every American campus. No campus is safe from such acts.

- *A plethora of new laws and regulations impacting higher education.* With over 2,400 federal, state, and local laws applying to higher education, colleges and universities are seeking new ways to operate to minimize the time and expense of their compliance responsibilities.

Risk used to be viewed as events that would result in a property or liability exposure, possibly leading to a financial loss. Such risks have typically been insurable. Managing these risks effectively created cost savings, as fewer accidents resulted in lower or flat insurance costs. ERM goes beyond insurable risks and includes:

- Competitive risk
- Market risks
- Financial risk
- Operational risk
- Technological risk
- Environmental risk
- Regulatory risk
- Litigation risk
- Political risk
- Strategic risk
- Business model risk

Reputation often appears on lists of ERM risks. One school of thought believes reputation is not a risk unto itself but rather a consequence of effective or ineffective risk management. In other words, reputation is always *at* risk but not *a risk*. The other school of thought considers reputation as a risk similar to any other risk. Under this approach, reputational risk exposures are events such as ethics breaches, fraud, and violation of academic standards. Under either school of thought, reputation must be well managed.

ERM takes into consideration how risks interrelate across campus and the degree to which those risks can impact efforts to achieve the institution’s strategic goals. It emphasizes the importance of measuring what really matters to the institution, the amount of risk the institution can tolerate, and what management efforts fit within its culture. ERM helps institutions to:

- Sustain competitive advantage
- Respond effectively when a significant event occurs
- Avoid financial surprises
- Effectively manage scarce resources
- Define risk appetite and tolerance levels
- Determine the effectiveness of existing risk management controls
- Improve risk assessments

- Increase management and business-unit accountability
- Allocate resources more effectively to address risk

Further, instead of having only a few dedicated personnel assigned to managing traditional risks on campus, ERM employs all staff to manage the risks for which they are responsible.

ERM is gaining importance in higher education. Developments in the business community, the financial rating agencies, and non-profit associations have drawn increasing attention to ERM among colleges and universities.

Business developments. Many trustees and campus leaders are knowledgeable about ERM from business settings, including experience with the Sarbanes-Oxley Act of 2002 (SOx). Although the act applies primarily to publicly-held companies, many trustees believe that components of it are essential to good practice in higher education. Sections of particular relevance to colleges and universities cover transparency of financial reports, corporate disclosure, board independence, accountability, and development of ethical operating standards.

The act requires enterprises to follow internal control rules; it does not specifically mention ERM. Nonetheless, many organizations have chosen to use COSO's enterprise risk management framework to help ensure overall compliance. The COSO standard is discussed in Step 8 of the road map.

More recently, the Securities and Exchange Commission issued guidance in 2007 placing greater emphasis on top-down risk assessment to further reduce an enterprise's financial risks. The SEC is developing new requirements on enterprise-wide risk and, in July 2009, the Commission proposed a rule requiring companies to disclose information about the board's role in managing overall risk.[2] The rule takes a broad view of risk, listing as examples credit risk, liquidity risk, and operational risk. Expected to be implemented in 2010, the rule underscores the directors' accountability for managing a company's material risks. Trustees and other leaders familiar with such developments may encourage a college or university to pursue an ERM initiative.

Financial rating agencies. As early as their 2004 rating cycles, the financial rating agencies began to understand and aggressively pursue the concept of evaluating the ERM programs of rated firms. The agencies looked to the COSO ERM framework. The first industries targeted were energy, financial services and other firms with large trading exposures, due in part to the magnitude of their financial risks as well as their ability to quantify those risks. The raters soon thereafter expressed a desire to expand the ERM evaluation process to the ratings of all industries, including the higher education sector. By 2006, raters were making exploratory inquiries at larger higher educational institutions. At a seminar in February 2008, sponsored by the Treasury Institute for Higher Education, analysts for Fitch, Moody's and Standard & Poor's indicated that their firms intended to include ERM factors in the rating process for higher education institutions. They estimated that it would be five years before institutions could expect to see meaningful evaluation of ERM in a rating.

In November, 2007, Standard & Poor's called for comments from the public about including the evaluation of ERM in the process of rating industries other than energy and financial services. Comments were due to Standard & Poor's no later than March, 2008. On May 8, 2008, the firm announced that it would phase in the inclusion of ERM factors in rating non-financial entities.

[2] The SEC proposed rule No. 33-9052 is available at **www.sec.gov**

Standard & Poor's evaluation process for ERM factors has been described as including three significant elements:

- Analysis of an entity's risk control practices, including its policies, infrastructure and methodology;
- Analysis of the firm's preparation for emerging risks; and,
- Analysis of the firm's strategic risk management.

Separately, Moody's Investor Service has commented that there is "a direct relationship between better-managed companies as measured by higher credit ratings and better performance as measured by fewer defaults on financial obligations.[3]

In their presentations on the subject (including in-person discussions, speeches, and published articles), the rating agencies have consistently struck a common theme of using ERM as an indicator of robust business practices to allow firms to avoid surprises. The agencies particularly emphasize avoiding "silo" risk management which creates the possibility that a convergence of diverse factors might multiply the effect of a given scenario on an institution's bottom line.

In its request for comments about including ERM analysis in non-financial firms' ratings, Standard & Poor's described the ratings as follows:

> "Companies that are considered "weak" on ERM are missing complete controls for one or more major risks, because the firm has limited capabilities to consistently identify, measure, and comprehensively manage risk exposures and thus, limit losses. Execution of its risk-management program is sporadic, and losses may be widespread according to a set of predetermined risk-/loss-tolerance guidelines. Risk and risk management may sometimes be considered in the firm's corporate judgment.
>
> Those companies considered "adequate" often manage risk in separate silos, but maintain complete control processes because the firm has capabilities to identify, measure, and manage most major risk exposures and losses. Firm loss-risk-tolerance guidelines are less developed. Unexpected losses are somewhat likely to occur, especially in areas beyond the scope of the existing ERM practices. Risk and risk management are often important considerations in the firm's corporate judgment.
>
> Companies that are "strong" demonstrate an enterprise-wide view of risks, but are still focused on loss control. These companies have control processes for major risks, thus giving them advantages due to lower expected losses in adverse times, as the firm can consistently identify, measure, and manage risk exposures and losses in predetermined tolerance guidelines. A strong ERM firm is unlikely to experience unexpected losses outside of its tolerance level. Risk and risk management are usually important considerations in the firm's corporate judgment.
>
> Companies that are considered "excellent" possess all of the characteristics of those scored "strong" and will also demonstrate risk/reward optimization. The firm has very well-developed capabilities to consistently identify, measure, and manage risk exposures and losses in the company's predetermined tolerance guidelines. Risk and risk management are always important

[3] "ERM: Rating Agencies Forcing the Issue", Michael J. Moody, March 2008 edition, Rough Notes

> considerations in the firm's corporate judgment. It is highly unlikely that the firm will experience losses outside of its risk tolerance.”[4]

Although the rating agencies have moved slowly over the past several years in evaluating higher education institutions’ ability to manage risks across the enterprise, ERM is clearly emerging as a concept that will command the attention of all institutions as a “best practice” and will be subject to scrutiny by the rating firms as their processes mature.

Many non-profit membership associations have devoted considerable time and resources to ERM in recent years. Their work underscores the powerful potential of ERM for colleges and universities.

Association of Governing Boards of Universities and Colleges (AGB). AGB is working to educate trustees and presidents on the value of ERM as a way to maximize opportunities and control adversity. Among other projects, AGB and United Educators issued a useful joint report titled “The State of Enterprise Risk Management at Colleges and Universities Today.”[5]

National Association of College and University Business Officers (NACUBO). For almost a decade, NACUBO has recognized the value of ERM to colleges and universities, encouraging business officers to initiate ERM on their campuses. James Morley, past President of NACUBO, has stated, “ERM’s holistic approach is the only way in which to manage the multitude of emerging risks on campus.” NACUBO has issued several significant reports, including “Meeting the Challenges of Enterprise Risk Management in Higher Education” and “Developing a Strategy to Manage ERM in Higher Education.”[6]

University Risk Management and Insurance Association (URMIA). URMIA has been in the forefront of educating its members in ERM with the goal of providing them with a better understanding of risk management and sharing resources on how to implement ERM. Among other efforts, URMIA has published a white paper on ERM in 2007 and included articles on ERM in the URMIA *Journal*.[7]

Risk and Insurance Management Society, Inc. (RIMS). Although not specifically oriented toward higher education, efforts of RIMS cannot be overlooked. In the past five years it has developed an electronic “Center of Excellence” for ERM practitioners. Resources include a library of ERM resources; a Risk Maturity Model useful for judging an entity’s development stage of ERM and devising steps to advance the process; an extensive resource library of articles on ERM; and links to various ERM standards and other resource sites. RIMS also offers numerous workshops and educational opportunities about ERM-related topics.[8]

[4] “Request For Comment: Enterprise Risk Management Analysis For Credit Ratings Of Nonfinancial Companies,” Standard & Poor’s; November 15, 2007

[5] To access a copy, visit www.agb.org/user-assets/documents/AGBUE_FINAL.pdf. For additional survey data used in the report, visit www.agb.org/user-assets/documents/AGBUE_REDACTED.pdf

[6] The reports may be downloaded, respectively, at www.nacubo.org/documents/business_topics/NACUBOriskmgmtWeb.pdf and www.nacubo.org/documents/business_topics/enterprisewide_risk.pdf

[7] Access to these resources is generally restricted to URMIA members. The white paper *ERM in Higher Education* can be downloaded at www.urmia.org/library/docs/reports/URMIA_ERM_White_Paper.pdf. Representative articles from the *URMIA Journal include “Enterprise Risk Management: A Fundamental Practice for Higher Education,” vol. 2003-2004 (p. 19) and “Moving Towards Enterprise Risk Management: A Basic Overview,” vol. 2003-2004 (p. 13). Visit* www.urmia.org/library/docs/2003URMIAJournalfinal.pdf

[8] The RIMS ERM resources, some of which are available to non-members, are collected at www.rims.org/ERM/Pages/default.aspx.

Associations of internal and external auditors. Leading organizations of internal and external auditors, including the Association of College and University Auditors (ACUA), have devoted considerable attention to ERM, addressing particularly its compliance-related aspects.

ERM resembles, at least in passing, other processes that may already exist on a campus. To a casual observer, ERM and traditional risk management appear to share some common elements. Both involve uncertainty and both can touch any unit of a college or university. Traditional risk management is, however, far narrower. It views risk as bad, seeks to protect an institution's property and financial assets from risk, and transfers risks to others through contractual risk transfer and the purchase of insurance or financing of risks. ERM accepts risk as a basic tenant of all operations and decisions and seeks to optimize outcomes. ERM seeks to view risk from the perspective of how risk(s) can affect the institution's overall objectives and strategic plans.

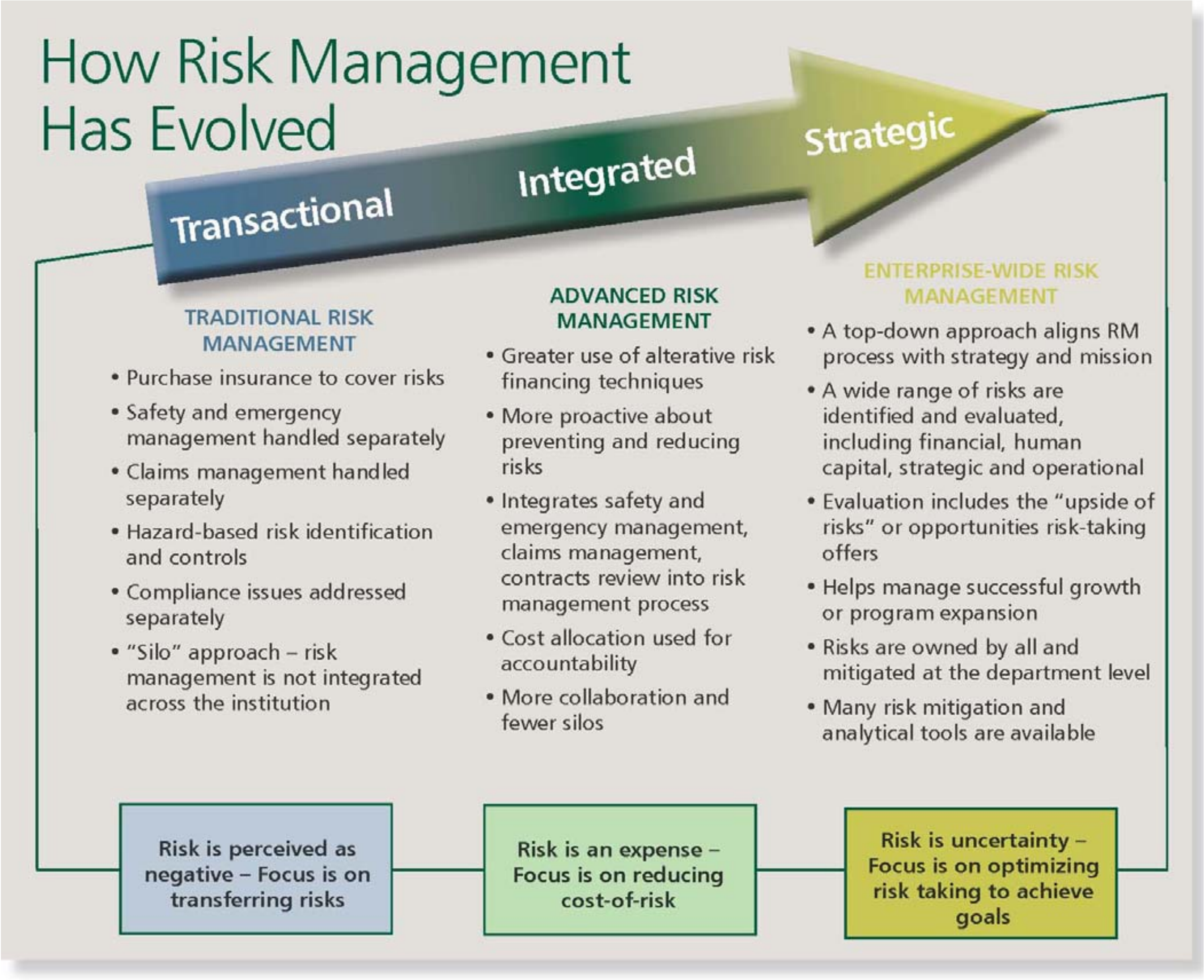
By broadening the concept and definition of risk in vital ways not contemplated by traditional risk management, ERM seeks to:

- Bring into consideration both the positive and negative aspects of risk
- View risk from the perspective of how risk(s) can affect the institution's overall objectives and strategic plans
- Promote collaboration with all departments and units and integrate multiple risk categories such as operational, financial, strategic, and hazard
- Align risk management processes with strategy and mission
- Help manage growth and effectively allocate resources
- Place responsibility for mitigating risks with the appropriate departments and individuals
- Enable the management of risks in the aggregate, offering a portfolio view of risks

A traditional risk management program can evolve into an advanced risk management approach. Advanced risk management focuses on controlling expenses associated with risk and it utilizes a variety of techniques to control those expenses. Advanced risk management can, over time, evolve into a broader ERM program. To do so requires commitment to making connections across campus and creating opportunities to have broader discussions about risk.

The following graph illustrates a typical evolutionary process towards ERM.[9]

[9] Graph provided by Dorothy Gjerdrum, Chair, U.S. Technical Advisory Group for Risk Management, International Standards Organization; Executive Director, Public Entity & Scholastic Division, Arthur J. Gallagher Risk Management Services, Inc.



How Risk Management Has Evolved

TRADITIONAL RISK MANAGEMENT

- Purchase insurance to cover risks
- Safety and emergency management handled separately
- Claims management handled separately
- Hazard-based risk identification and controls
- Compliance issues addressed separately
- "Silo" approach – risk management is not integrated across the institution

ADVANCED RISK MANAGEMENT

- Greater use of alterative risk financing techniques
- More proactive about preventing and reducing risks
- Integrates safety and emergency management, claims management, contracts review into risk management process
- Cost allocation used for accountability
- More collaboration and fewer silos

ENTERPRISE-WIDE RISK MANAGEMENT

- A top-down approach aligns RM process with strategy and mission
- A wide range of risks are identified and evaluated, including financial, human capital, strategic and operational
- Evaluation includes the "upside of risks" or opportunities risk-taking offers
- Helps manage successful growth or program expansion
- Risks are owned by all and mitigated at the department level
- Many risk mitigation and analytical tools are available

Risk is perceived as negative – Focus is on transferring risks

Risk is an expense – Focus is on reducing cost-of-risk

Risk is uncertainty – Focus is on optimizing risk taking to achieve goals

The best situation is one in which the top leaders promote and endorse an ERM initiative. Top-level support allows a risk management program at any stage of development to jump directly to ERM, without evolving through the various stages or phases.

ERM also shares some common characteristics with internal audit and compliance. Audit and compliance reviews assess whether campus departments are following institutional policies and meeting legal obligations. Deficiencies can undermine the entire institution and hinder efforts at progress. While some ERM initiatives narrowly focus only on compliance, many are broader. ERM in its most effective form looks at changing circumstances, new opportunities, and all strategic, financial, and operational decisions. How well is a college prepared for an expected decline in the number of 18 year olds? Has the institution discussed the amount of risk it will accept or tolerate? These are more matters of strategy and judgment than compliance with policies and laws. While compliance is a component of ERM, the best ERM programs have a broader scope.

ERM thus reaches beyond both traditional risk management and internal audit and compliance. Given its breadth, ERM merits the attention of top-level leaders. Governing board members are natural allies. They bear fiduciary responsibility for the institution as a whole. An effective board focuses on strategic opportunities that will enhance the mission and sustain the institution's competiveness. Trustees' interest in ERM stems, in part, from the growing need to assure key constituencies that the institution is effectively managing all of its risk. The President (or chancellor) is another natural ally. Because ERM is a component of leading and managing a college or university, the president ideally should be the promoter, if not the initiator, of ERM on campus. By assuming leadership of ERM, the president places it at a strategic level. Explicit commitment from the governing board and president provides the strongest foundation for an ERM program.

Many risk managers are enthusiastic about ERM and have successfully lead ERM implementation efforts on their campuses. ERM allows risk managers to address the larger needs of their institutions, thus creating more value and upgrading their functions. Sometimes, though, higher education risk managers remain as supporters of ERM rather than its leaders. Other important supporters include the president's executive cabinet (e.g., CFO, provost, vice presidents, general counsel, and deans) who provide operational clout to an ERM initiative.

Other campus administrators who play roles in traditional risk management are also natural allies of ERM. They may include the IT director, student housing director, director of security, and facilities director. In some instances, a risk manager has successfully partnered with an internal auditor or general counsel, or both, to lead ERM efforts. Their combined success typically surpasses the results that can be achieved in isolation. Ultimate responsibility for ERM will, however, normally remain with the president and the board.

While support from the board and key administrators is helpful, it is not essential. The Think Tank participants observed that an ERM initiative may begin from the "top-down" or the "bottom-up." They then concluded that the latter category is better described as "middle-up" when the initial champion is in a middle management role.

There are times when a "middle-up" ERM initiative can get underway more expeditiously than one awaiting direction from the top. It would typically begin with one or more pilot projects. These would involve several departments and integrate a broad definition of risk into decision making. A pilot project can, over time, lead to more comprehensive endeavors. A successful middle-up initiative can build upper-level support, as the ERM champion demonstrates ERM's worth to key administrators and the board. A middle-up initiative helps traditional risk management evolve into a more advanced form.

A "middle-up" approach might sometimes be more enduring than a "top down" one. At many institutions, top administrative positions turn over more rapidly than middle management. Thus, an ERM initiative in the hands of, say, a risk manager may be more sustainable than one headed by a president who is replaced after several years.

The Road Map for a Phased Approach to Drive the ERM Process

We turn now to the heart of the matter, a practical road map for implementing ERM. The road map is grouped into four phases: building a case for ERM; building an ERM foundation; implementation; and sustaining your ERM program. Under each phase you will find several steps. A chart compiling all the steps appears as Appendix A.

The road map is designed for institutions of all types – large, small, public, and private. The steps should be adapted to fit the circumstances. One key variable is whether the ERM initiative originates from the top of the institution or its middle. If the governing board or president is championing ERM, the process proceeds slightly differently than if a middle manager initiates it. Step 4, for example, is "Present the case." The governing board or president may usefully prepare a written justification to help guide the staff with primary responsibility for implementation. A middle manager writing a case statement, in contrast, will want to include reasons for the board and president to embrace ERM.

Some of the steps are sequential, while others should occur throughout the process. Step 20, on communication, reporting, and monitoring, should not be saved until the end. Those functions need to occur continuously during ERM. Keep in mind that there is no single best approach. Adapt the phases and steps to your institution's unique culture.

Phase One: Building a Case for ERM

Phase One surveys the institution's situation, including its plans, environment, culture, existing risk management processes, goals, and objectives. From these factors, a case statement for ERM is prepared. The case statement should present a compelling story of the benefits that ERM can bring to the institution.

Step 1: Understand the institution's plans, environment, and culture

Where does the institution want to go? On what key initiatives is it focusing? Look first at the campus strategic plan. The plan may aim for expansion of existing programs or the creation of new ones. It may stress globalization, community service, or technology transfer. The institution may want to improve its academic rigor, student body diversity, or scientific research. History matters. A college that has not met its enrollment targets may address financial risks differently from another with sufficient resources. A university that recently suffered a shooting death may place higher priority on campus security than one that has not. There are many directions in which a college or university might want to go.

After reading the strategic plan, review other documents and statements that reflect the institutional mission, strategies, plans, and risks. A mid-level ERM champion may want to review the following risk-identifying documents.

- Organizational charts for the institution, business units, and academic departments
- Key management documents such as accreditation reports
- Board meeting material and minutes
- Student and employee handbooks

- Environmental health and safety and other related policies and procedures
- Research, technology transfer, and intellectual property policies and procedures
- Business continuity plans
- Available financial reports for the three most recent years
- Current annual and long-range budgets
- Information on grant sources, types, and amounts
- Clery Act information and incident reports
- List of contracted vendors (e.g. food service)
- IT security and usage policies, including software licenses
- Institutional review board meeting agendas and minutes
- Radiation Safety Committee meeting agendas and minutes
- Animal Care committee meeting agendas and minutes
- External audit reports and management recommendations
- Internal audit reports

Such documents, in the aggregate, provide a picture of the institution's plans, culture, and risks.

Step 2: Determine the status of your existing risk management processes

Traditional risk management exists on every campus, whether or not called by that name. Someone buys insurance and someone repairs broken steps. Pose the following questions to develop a snapshot of the extent risk management is already taking place on your campus.

- What risk information is being generated and by whom? How is it acted upon?
- Does "risk" have a common meaning across campus?
- Who monitors the emerging risks of the external world, such as proposed regulatory and political changes, social trends, and student demographics?
- If you have an internal audit program, what risks has it identified? Does internal audit review or discuss audit findings with risk management?

- If your institution does not have internal audit function, who monitors risk and compliance?
- What departments have been particularly supportive of risk management initiatives and would support a cross-departmental review of risks emanating from their activities?

A summary of these findings will help to describe existing risk management structures in the case statement to support ERM. It will also help to define the gap between current operations and what is needed or desired.

Step 3: State your goals and objectives

Consider whether the institution is ready for full ERM implementation or whether more limited initiatives may be more appropriate. A limited approach might begin within one or more departments which have ownership of a key strategic initiative and have been identified as supportive of risk management initiatives.

Consider why an ERM process would be beneficial at your college or university and tie the benefits into your institution’s vision or mission statement. For example:

> “XYZ University’s mission is to improve the lives of our students by combining a classical liberal arts education and life skills to create a balance between technology and the natural world through research.”

To assure the institution’s mission is successfully achieved with the least possible risk, ERM goals might include:

- Embedding a risk-based decision making process across campus
- Identifying and assessing risks
- Assigning ownership of risk
- Breaking down barriers between departments
- Identifying risk drivers and causal relationships
- Implementing risk treatment options
- Establishing exposure and trend tracking criteria
- Effectively managing risk/reward opportunities

Attach objectives to each of the identified ERM goals. Explain how the objectives will help to more productively achieve the goals. For example:

ERM Goal: Embedding a risk-based decision making process specific to research activities across campus

Objectives: By completing the following objectives, we will embed a risk-based decision making process across campus, because of increased understanding and buy-in from staff and faculty.

1. Identify those risks that are most material to the institution’s mission and strategic plan

2. Analyze existing risk management strategies and techniques used to manage those risks

3. Determine what, if anything, more can be done to better manage risks

4. Incorporate management techniques into training programs for risk owners

5. Create ERM “tools” to aid employees in conducting their own risk assessments of existing and any new/proposed research activities

6. Plan and deliver six cross-campus training sessions on ERM during fall semester

7. Circle back and interview all training participants after six months to determine information retention, and identify refresher course needs

This process can be applied to each implementation step of the institution’s plan to achieve its mission. To do this most effectively, you will need to understand the institution’s strategic initiatives, its environment, and its practices regarding risk ownership and mitigation.

Step 4: Present the case

If a case can be made for initiating an ERM process on campus, prepare and present a case statement as an executive level briefing of your findings, priorities and recommended strategies for implementing ERM. In addition to explaining how ERM will benefit the institution, the case statement may include some or all of the following points:

- A statement as to why ERM is needed or desired

- A description on how well the institution is positioned to implement ERM

- A statement on how ERM will fit in within the institution’s culture

- The potential value of ERM as articulated by associations such as AGB, NACUBO, and URMIA

- The value of ERM in the institution’s financial ratings

- Examples of other institutions that have successfully implemented ERM programs

- Examples of the greatest risks to the institution. The report can highlight the institution’s risks by operating unit or geographical location illustrating how risks crossover from one operating area to another, including where insurance can be aligned with the risks and where insurance isn’t feasible.

- A description of existing capabilities and gaps for managing risks. Make the case, as needed, for increased staffing to better integrate risk management throughout the institution

- Scenario analyses illustrating the upside and downside impacts of the societal, technological, environmental, economic, and political changes associated with each of the institution's strategic initiatives

- What human and financial resources will be needed

- Who will lead the process

- A description of the anticipated challenges. These might include barriers to success, why and how the process may be opposed, and strategies to minimize the challenges.

- How success will be measured

For samples of case statements and governing board presentations on ERM, visit the websites of the higher education ERM programs listed in Appendix A.[10]

Step 5: Obtain top-level commitment, support, and participation

If possible, have the chair of the board of trustees or president state in writing a commitment to managing risk as a component of achieving institutional objectives. The governing board might adopt a resolution, or the president might distribute a policy statement. Messages from the top help sustain momentum and provide authority to act.

Another place for a written statement is the institution's strategic plan. For example, the 2006 - 2009 strategic plan for The Pennsylvania State University included a strategic objective to "identify, quantify, and mitigate risks across the University within its system of policies and procedures, finance, human resources, physical assets, and operations."

As part of the process of embedding risk management in all parts of the institution, it helps to include in the mission statement provided by the board or president an explicit endorsement of ERM. The three basic elements of an effective statement of support include:

1) Senior leadership's commitment to the process

2) Expectations of senior leadership in the success of the ERM initiative

3) Expected commitment of staff and faculty involvement

Use the written statement as evidence of support and authority to win over skeptics and as a reminder of the program's overall goals. As appropriate, refer to such top-level statements in subsequent ERM reports.

Remember that if senior level support is not attainable for an institutional ERM process, you can still begin to grow the process organically by building on existing risk management efforts. Select one or two cooperative departments, get buy-in, and enlist them in risk identification and mitigation projects. Seek partnerships, such as with the compliance officer, to gain clout and cooperation within selected departments that could most benefit from risk management attention. Focusing on a few key

[10] For an ERM presentation made to the University of Washington governing board, refer to pages 88-106 in the materials at www.washington.edu/regents/meetings/minutes/2007/2feb.pdf.

achievements may be better than trying to implement a too-ambitious, comprehensive program. Do not give up on ERM just because top-level support is lacking. Take the initiative, start at the department level, and build on small successes. With time, commitment, and results, you can build support for implementing a broader approach.

Step	Phase One: Building a Case for ERM	Start Date	Target Finish
1	Understand the institution's plans, environment, and culture		
2	Determine the status of your existing risk management processes		
3	State your goals and objectives		
4	Present the case		
5	Obtain top-level commitment, support, and participation		

Phase Two: Building an ERM Foundation

Phase Two sets the foundation on which to build, embed, and sustain an ERM process. It also sets the scope and structure for the project.

Step 6: Name an ERM leader

When an ERM initiative starts at the top, the president or chancellor often appoints the process leader. A recent survey of ERM in higher education asked to whom the governing board or president had assigned primary responsibility for institutional risk management. The results from 467 respondents identified several major roles. (Multiple answers were permitted, so the total exceeds 100 %.)[11]

❖ Financial officer	50%
❖ President	32%
❖ Chief risk officer	7%
❖ Chief legal officer	6%
❖ Other	15%

As the survey results show, a risk manager may, or may not, lead an ERM initiative. The broad scope of ERM requires skills and vision that a risk manager may not have acquired. The ERM leader is often appointed from an existing position rather than from outside the institution. Internal candidates are most familiar with the institution and have already established relationships with key individuals. They know how to get things done, which is invaluable for large-scale initiatives. A new hire, in contrast, may bring a fresh perspective, different skills, and a clean slate not already overburdened with other responsibilities.

[11] "*The State of Enterprise Risk Management at Colleges and Universities Today*," by the Association of Governing Boards of Universities and Colleges and United Educators (2009). The full text is available at www.agb.org/wmspage.cfm?parm1=1596

Chief Risk Officers (CROs) have become more common since the enactment of SOx. A CRO is a senior-level administrator accountable for assuring effective oversight of risk managing strategic opportunities and enabling the institution to balance risk and reward. The CRO often reports to the executive committee of the governing board, the president, or the treasurer.

Professional associations for internal auditors have actively promoted ERM, but should an internal auditor lead an ERM initiative? The components of an internal auditor's role are (i) to provide objective assurance of a college or university's effectiveness in utilizing its business controls and (ii) to ensure compliance with policies, plans, procedures, laws, and regulations. Assuming responsibility for ERM operations may compromise the auditor's independent judgment.

When an initiative begins with a mid-level champion such as the risk manager or business officer, that individual may voluntarily assume the leadership responsibility. Whatever the position, useful attributes in an ERM leader include:

- Strong working knowledge of the institution's major functions and structures

- Good project management skills

- Effective communication and relationship-building skills

- Knowledge about ERM, or an interest in learning

Launching ERM throughout a Higher Education System

The Maricopa County Community College District ERM initiative started with a strong mandate from the Chancellor. After a planning period, the ERM project was rolled out simultaneously to all 10 colleges in the district. The ERM committee includes representatives from both the district office and the individual campuses. One campus president serves on the committee.

The ERM initiative was named the Maricopa Integrated Risk Assessment project, with the acronym MIRA. Mira is more than an acronym for their project. In Spanish it means "to look." The tagline for the MIRA logo is "a new way of looking at risk." MIRA is more than five years old and has created many useful reports and tools, described elsewhere in this report.[1]

To implement ERM in a higher education system, one can either begin simultaneously on all campuses, as Maricopa did, or start an ERM project on a pilot basis and then expand it to all institutions, as the University of Wisconsin is doing.

Step 7: Plan your project and create a timeline

Planning sets the compass to a defined endpoint. As Lewis Carroll said, "If you don't know where you are going, any road will get you there." The route must be tailored to the needs of those along for the ride. Planning typically includes the following elements.

a) *Involve the right people in the planning process.* Get input from everyone potentially involved in the implementation process. They should review the final draft and approve the plan.

b) *Define the goals.* Establish the outcomes you seek from the ERM process. In goal setting, some people rely on the "SMART" method. SMART, an acronym, stands for the following concepts:

- *Specific:* The more specific the goal, the more realistically it can be achieved
- *Measurable:* The desired outcomes of any goal should be measurable
- *Acceptable:* To be achievable, goals must be acceptable to all those involved with or affected by the goal's outcomes

- *Realistic:* Even if the goal is specific, measurable, and acceptable, you won’t get there unless it is also realistic
- *Time frame:* Time frames focus the attention of participants

c) *Define objectives.* Often labeled “milestones” or “tasks,” objectives are the steps necessary to accomplish the goals.

d) *Identify needed resources*. Resources include budgets, people, materials, and technology.

e) *Assign responsibilities for achieving various goals and objectives*. Assignments should also include deadlines for each responsibility.

f) *Communicate the plan.* Communicate your ERM mission and goals. Let the campus community know about the plan and give them reason to get onboard with it.

g) *Acknowledge completion of goals and objectives.* Too often this step is ignored. Recognizing the accomplishment of a goal or objective can provide personal recognition and enhance motivation.

Step 8: Select or design an ERM framework that best fits the institution’s goals and culture

Many organizations have promulgated formal standards for implementing ERM. Most have been motivated by the need to improve corporate governance. Below we describe the most prominent standards. It is typical for international standards to refer only to “risk management,” not “ERM.” ERM, as something different than risk management, is a uniquely American concept.

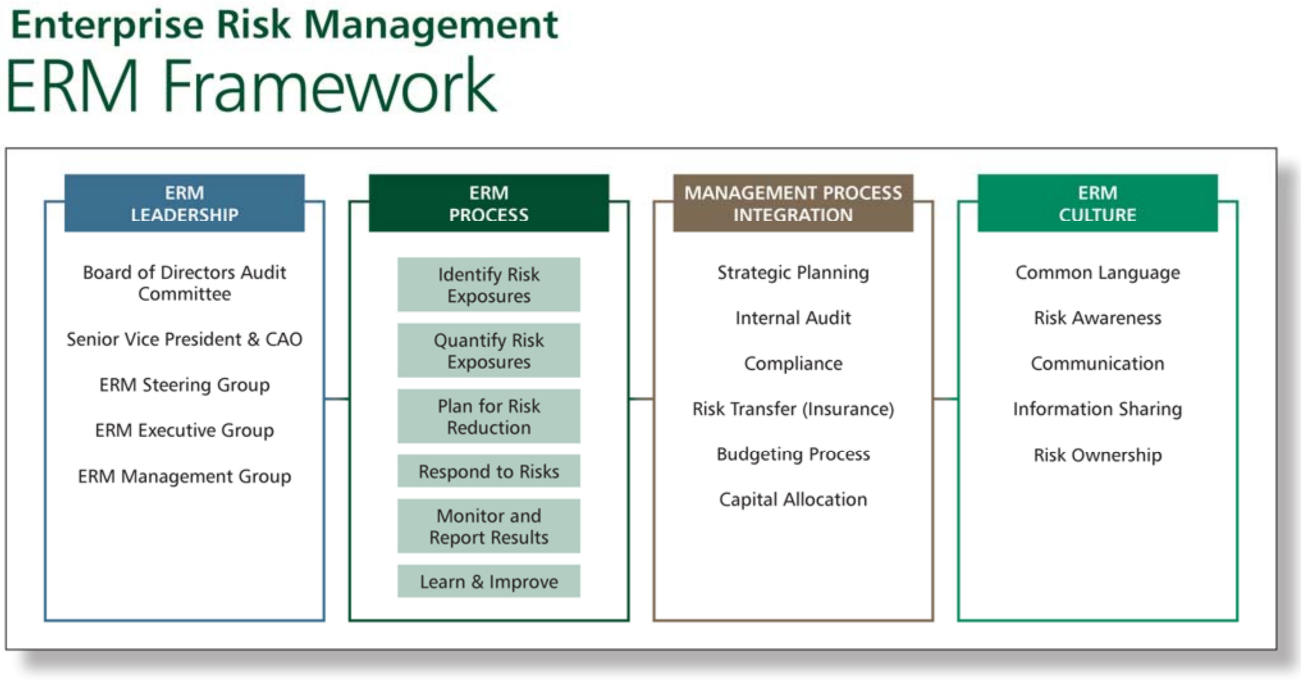
While standards can provide guidance on creating an effective campus ERM program, it is not necessary to rely explicitly on any one standard. Many written materials, including this report, incorporate the best parts of different standards.

Should you decide to base your campus ERM efforts on an existing standard, be sure to refer back to it often. It can provide ideas and guidance on maintaining and improving your program over time. You may prefer to select the most useful elements from various formal standards to create your own ERM framework.

One Approach to ERM Standards

A Think Tank participant observed, “The ERM process at my institution is growing organically, building on processes that were developed for other reasons and directed to addressing institutional concerns. My advice to others is that when it comes to risk, consider what the institution needs and then tackle that without trying to comply with some standard unless and until a higher education standard develops.”

The following is a framework that Georgetown University follows:[12]



Enterprise Risk Management

ERM Framework

ERM LEADERSHIP	ERM PROCESS	MANAGEMENT PROCESS INTEGRATION	ERM CULTURE
Board of Directors Audit Committee	Identify Risk Exposures	Strategic Planning	Common Language
Senior Vice President & CAO	Quantify Risk Exposures	Internal Audit	Risk Awareness
ERM Steering Group	Plan for Risk Reduction	Compliance	Communication
ERM Executive Group	Respond to Risks	Risk Transfer (Insurance)	Information Sharing
ERM Management Group	Monitor and Report Results	Budgeting Process	Risk Ownership
	Learn & Improve	Capital Allocation	

The following are among the most prominent standard setting organizations.

International Organization for Standardization (ISO). The ISO 31000 Risk Management – Principles and Guidelines are applicable to any organization and to all risks. It emphasizes the continuous activities of monitoring, review, communication, and consultation. Earlier standards did not fit multinational organizations well, but ISO 31000 is sufficiently flexible to meet this need. It supports a five-step risk management process and relies on management controls rather than internal controls. The ISO risk management standard is a variation of an earlier standard adopted by the Standards Australia/Standards New Zealand Joint Technical Committee on Risk Management, discussed below. The ISO standard is now replacing the Australia/New Zealand approach.[13]

Australia-New Zealand Standard. The Australia-New Zealand standard, known as "Risk Management Guidelines AS/NZS 4360:2004," was developed by a joint technical committee of representatives from for-profit and non-profit groups in Australia and New Zealand. The standard is designed for use in any type of organization. It offers a nine-step program for implementing ERM.[14]

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is a voluntary private sector organization.[15] It is dedicated to helping improve the quality of financial reporting through business ethics, effective external controls, and corporate governance. 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. Through the

[12] Used with permission, the ERM Framework is courtesy of Georgetown University.

[13] To learn more about ISO 31000, go to www.iso.org/iso/catalogue_detail.htm?csnumber=43170

[14] To learn more about AS/NZD-4360:2004, go to www.mrcmekong.org/download/programmes/ep/Aust_Standards_4360-2004.pdf

[15] To learn more about COSO, go to www.erm.coso.org

work of internal auditors, COSO produced the original ERM framework in 1992 and it was finalized in its current form in 2002. Its standards are focused on compliance and based on controls.[16]

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.”

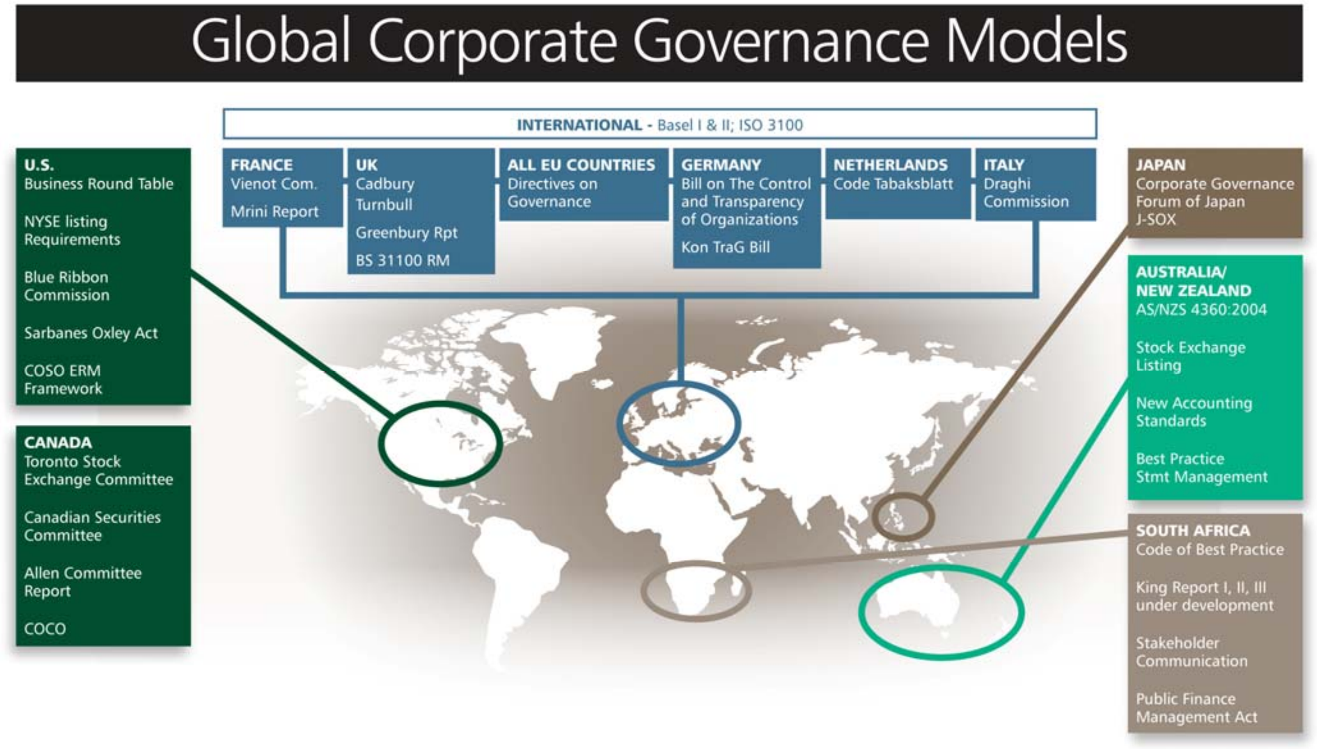
COSO provides a model to achieve its recommended process that includes:

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

Other standards include a British model and, for banking regulation, the Basel II Accord. Most groups that create risk management standards sell them and then, for an additional fee, provide certification services.

As noted above, formal ERM standards have been designed largely to improve corporate governance.

[16] The National Association of College and University Business Officers, in collaboration with PriceWaterhouseCoopers, adapted the COSO framework to higher education in a 2001 study, *“Developing a Strategy to Manage Enterprise-wide Risk in Higher Education.”*



Global Corporate Governance Models

INTERNATIONAL - Basel I & II; ISO 3100

FRANCE
Vienot Com.
Mrini Report

UK
Cadbury
Turnbull
Greenbury Rpt
BS 31100 RM

ALL EU COUNTRIES
Directives on Governance

GERMANY
Bill on The Control and Transparency of Organizations
Kon TraG Bill

NETHERLANDS
Code Tabaksblatt

ITALY
Draghi Commission

U.S.
Business Round Table
NYSE listing Requirements
Blue Ribbon Commission
Sarbanes Oxley Act
COSO ERM Framework

CANADA
Toronto Stock Exchange Committee
Canadian Securities Committee
Allen Committee Report
COCO

JAPAN
Corporate Governance Forum of Japan
J-SOX

AUSTRALIA/ NEW ZEALAND
AS/NZS 4360:2004
Stock Exchange Listing
New Accounting Standards
Best Practice Stmt Management

SOUTH AFRICA
Code of Best Practice
King Report I, II, III under development
Stakeholder Communication
Public Finance Management Act

Step 9: Create a cross-functional Risk Council

The Risk Council is the internal group that reports to senior management. (While different institutions use different names, such as the ERM Advisory Committee, we will use Risk Council for ease of reference.) The Risk Council will typically draw from all major divisions of the institution. These may include the office of the provost, finance, risk management, legal office, student affairs, information technology, and internal audit or compliance. Other departmental representatives may come from athletics, environmental health and safety, human resources, international programs, public safety, and university relations.

It is important for the risk manager to have a seat on the Risk Council. After all, he or she is the person on campus most experienced in risk identification and risk mitigation techniques. The risk manager often serves as the knowledge expert for process on the Council.

The Risk Council becomes the coordinating body of those on campus who have institutional responsibility for managing risk.

One advantage of a cross-functional committee to address risk is that it brings people with in-depth and practical knowledge of specific risks together with those most familiar with institutional policies, procedures, and resources. Another advantage is the cooperation that emerges among staff and faculty as they work together on mitigating risks to the institution’s advantage. Moreover, given their positions on campus, the members of the Council will have sufficient clout to ensure that issues are investigated and resolved. The committee should meet on a regular basis to address risk issues. The chair should report on the Council’s activities to the board or senior leadership.

Some institutions choose to appoint a second higher-level ERM oversight committee. This committee's functions can include monitoring the Risk Council's work and providing additional resources to implement needed action steps. An oversight committee is typically small, perhaps three or four people. It might include the CFO, provost, or other representatives from the institution's executive cabinet. If the president is not leading the ERM program, he or she might sit on an ERM oversight committee. If an oversight committee exists, it will typically provide the governing board, or relevant board committee, with regular reports on the ERM process.

Step 10: Create a mission and goals statement for the Risk Council

A mission and goals statement serves as the driving force behind the success of the Risk Council. It is a brief written statement describing the Council's purpose and goals; it provides direction, describes the Council's activities, and guides decision making. Additional benefits of a well-crafted mission statement include helping committee members focus solely on those responsibilities assigned to them and defining measurable outcomes.

It is important that the mission statement receive high visibility on campus. When people see it often, they will be reminded of the commitment the institution has made to the ERM process.

Here are two examples of college and university Risk Council mission statements:

> The Enterprise Risk Management Advisory Committee will advise the president's cabinet regarding a structured approach to identifying and managing the institution's risks. The Committee will assist in broadcasting these risk strategies and help hold the stake holders accountable for ownership of identified risks. They will be charged with integrating risk considerations into key operational and strategic decision-making. The committee will draft a risk appetite statement for review and approval by the president's cabinet.[17]

At a multi-campus system, the Risk Council is charged with the responsibilities to:

- Promote and advance risk awareness and understanding through discussions and training forums with other councils and employee groups.
- Provide leadership in the identification, resolution, and monitoring of cross-organizational issues related to risk.
- Assist in the elimination of functional, cultural, and department barriers in dealing with risks.
- Construct a risk assessment methodology for continuously identifying risks, both internal and external, across the system.
- Assist in the development of mitigation strategies.
- Serve as advisors to the risk manager by contributing ideas and feedback on risk management initiatives.
- Provide reports to the Governing Board, Executive Council, Strategic Planning Council, Capital Planning Council, and Employee Groups annually and as requested.

[17] Ohio State University, September 2008. www.busfin.ohio-state.edu/FileStore/Risk_AdvCmt.pdf

- Monitor the progress of the ERM project.
- Create risk assessment teams at each college.[18]

A more generic statement might read, “The Enterprise Risk Management Council collaborates to identify and manage the university’s risks. The Council identifies risk management strategies and is charged with communicating them to each member’s respective areas so that appropriate persons will take ownership. The Council will establish, with a balanced view between understanding the upside and downside of risks, a process that mitigates and controls uncertainties and manages opportunities on campus. The Council reports to the President.”

Step 11: Develop a shared vocabulary and definitions

A common risk language accepted across campus is critical to creating a risk culture, taking risks, and sharing in risk management. It will guide how risks are identified and managed**.**

People in different campus roles may define risk differently. The president may think of risk as involving risks to the institution’s reputation and donor support. A finance officer may think first of cash flow and investment risks. Internal audit will think of compliance risks, and a traditionally-focused risk manager will think of hazards to eliminate, insure against, or assume.

For this reason, the Risk Council will need to develop and promote a common risk vocabulary to establish a mutual understanding of the words, terms, and phrases that describe the ERM process. The vocabulary and definitions will also need to fit the institutional culture**.** It may be difficult, for example, to promote the idea that risk is “the effect of uncertainty on objectives,” as the term is generally used in ERM. The phrase “opportunities and risks” might resonate more on some campuses. The acronym ERM may have been appropriated already for another use, such as “electronic records management.” (Check with the head librarian.) Other terms to define might include compliance, heat map or risk map, materiality, mitigation, risk appetite, risk owner, and risk treatment.

For examples of risk terms and definitions, see the end of this document for the *Maricopa County Community College District’s Risk Lexicon.*

STEP	Phase Two: Building an ERM Foundation	Start Date	Target Finish
6	Name a project leader		
7	Plan your project and incorporate a timeline		
8	Select or design an ERM framework that best fits the institution’s goals and campus culture		
9	Create a cross-functional Risk Council		
10	Create a mission and goals statement for the Risk Council		
11	Develop a shared risk vocabulary and definitions		

[18] Maricopa County Community College District, Charge to MIRA Project Committee, 2004, reaffirmed 2005 and 2006. www.maricopa.edu/mira/charge.php. The University of North Carolina at Chapel Hill has implemented an ERM program across its campus, which includes an ERM Advisory Committee. To learn more about the mission of UNC’s ERM Advisory Committee, the membership of the committee, and to read a description of its duties and responsibilities, go to http://www.unc.edu/risk/erm.htm.

Phase Three: Implementation

The implementation phase involves risk identification, risk evaluation, and taking action in priority areas.

Step 12: Develop a risk portfolio

The next step is to develop a portfolio of the institution's risks. The Risk Council might begin by compiling an exhaustive list and then paring it down by prioritizing.

Planning documents, reports, and other documents reviewed in Step 1 will suggest items for the risk portfolio. You can also elicit ideas through techniques such as interviews, surveys, SWOT[19] analysis, and workshops. Interviews of key personnel may be conducted by internal audit or risk management staff**,** or external consultants can be engaged for purposes of objectivity.

Evaluate both internal and external environments, and track local and state trends and trends in higher education that could affect the institution. For example, is the state attorney general investigating fraud? Might a significant number of faculty retire in 10 years? Do students want to graduate in three years rather than four? One research university collected information on matters of compliance, including major fines, penalties, and repayments that similar institutions had experienced. Potential problems included medical billing errors, misuse of federal grants, and payments for discrimination claims.

The initial risk portfolio may be huge. Emory University, for example, identified 555 issues in its initial analysis.[20] The next step, necessarily, is extracting from the large inventory those risks that are material. A compilation of hundreds of risks may be overwhelming to prioritize and mitigate. A Risk Council may become mired in worry over unrelated and unmanageable risks. As Keith Shakespeare, Chief Operating Officer for the Canadian Universities Reciprocal Insurance Exchange (CURIE), has explained, "It is not sufficient to have a laundry list of risks – no institution can afford to control all risks."[21]

If you think your efforts may stall at this point, adopt a more limited approach. You could, for example, elicit risk concerns just from the governing board and senior leadership, assembling a manageable portfolio of the risks they perceive. The recent report "The State of Risk Management at Colleges and Universities Today" is directed toward that audience. Designed for use by the governing board and the president, the report includes worksheets on risk identification and ranking. The worksheets group risks by operational area. A separate worksheet covers each of the following operations: academic affairs, board governance, compliance, external relations, facilities, finance, human resources, information technology, research, and student affairs.

[19] SWOT is a method used to analyze the Strengths, Weaknesses, Opportunities, and Threats that could impact an institution's objectives. It involves identifying factors that are advantageous or disadvantageous to achieving each objective.

[20] "Emory University: ERM in Ten Easy Steps," Edie Murphree and Steve Sencer, February 2008 presentation at the Treasury Institute for Higher Education, Available at www.treasuryinstitute.org/resourcelibrary/Symposium_2008/handouts/25.pdf

[21] CURIE Newsletter, Volume 14 Issue 3; September 2003; "University Risk Control Starts with Risk Assessment" by Keith Shakespeare.

The worksheet for facilities, for example, includes:

- Accessibility
- Auto/Fleet
- Disaster preparedness
- Maintenance and condition
- Outsourcing
- Pollution
- Safety
- Security
- Transportation

Users are invited to add their own ideas. Additional topics for facilities might include, among many others, strategic issues of under-used facilities or overcrowding. The worksheets invite users to rate the urgency of each area and, for the most urgent risks, assign an individual to address each one. Published jointly by the Association of Governing Boards of Colleges and Universities and United Educators, the full report may be downloaded from AGB's web site.[22]

Another, more limited approach is to concentrate on identifying all the risks in one or more selected departments such as, for example, chemistry. Address significant issues within the targeted area. This approach, however, leaves serious risks in other departments unevaluated and possibly unmanaged. Also, clusters of risk in one department do not necessarily rise to the strategic or material levels, nor do they typically garner attention outside of organizational silos. Yet the potential risk of personal or environmental exposure to a hazardous material may extend far beyond the chemistry department. [23]

There is no magic number for your final priorities. From the dozens or hundreds of issues identified, you might select 5, 20, or 75. The limit is the number of issues the institution can realistically address at one time and that merit immediate attention. Find the risks that potentially impact the institution's ability to meet its strategic objectives. Examples include faculty recruitment, protection of intellectual property, endowment management, contagious diseases, and NCAA compliance. A portfolio approach illustrates the interconnected nature of risks. Managing one risk can change the likelihood or severity of another. The interconnectedness of risks is a key element of ERM.

Each area selected for inclusion should be *material* to the institution. As one Think Tank participant stated, "The only risks that should be on the list are those that could impact the institution over a selected dollar threshold or have a significant impact on reputation."

While the word material has many different definitions, some of them quite technical, we use it to mean how important something is to the institution's ongoing operation and future success.[24] Define what materiality means at your institution when you create your risk vocabulary under Step 11.

[22] http://www.agb.org/user-assets/documents/AGBUE_FINAL.pdf

[23] From the perspective of hazards, a chemistry student who lives on campus may carry dangerous materials across campus to complete a class assignment in his or her dorm room. A fellow student may be planning to do something similar in his or her off-campus apartment. On campuses with multiple locations, research faculty members have even been known to transport radiological and bio-hazardous materials in their personal vehicles from classrooms to off-site laboratories and satellite research sites.

[24] Under SOx, for example, materiality refers to a formula that a company uses to determine exceptions to key financial control processes.

As Keith Shakespeare has written, “Since most risks will be tolerated or ignored, don’t waste time and money analyzing insignificant risks.”[25] To help gauge whether a risk is material, consider the following five questions:

1. Does the risk have a significant financial, operational, or strategic impact on the institution?
2. Is the risk key to the success of the strategic plan?
3. Does the risk affect any activity routinely reported by the press which compares peer institutions, such as number of qualified applicants, endowment returns, research grants awards, etc?
4. Is the risk a matter of serious concern for institutional stakeholders; for example the controversy surrounding animal use in research?
5. Is the risk a part of the institution’s routine operations, for example hazardous waste generation from undergraduate and research labs?

Whatever the path, the endpoint should be a portfolio of risks that are material to the institution’s current operations and long-range plans.

Exploring Materiality at the University of Wisconsin

The University of Wisconsin System has begun pilot ERM programs at two of its institutions, the University of Wisconsin Superior and the University of Wisconsin Oshkosh. Cross-functional teams have been developed at those universities, and goals and objectives have been established. An initial challenge for the teams is identifying the points at which certain changes, such as declines in revenue, enrollment, or graduation rates become critical or material to the achievement of identified goals and objectives. A long-term objective is to link campus ERM initiatives to system-wide ones.

The pilot program began at the system level, with a self-initiated review of the University of Wisconsin System administration. The review provided ideas on many subjects including ways to validate risk and assess the relative impact of risks, as well as likely hurdles to ERM implementation. After the review, the UW System decided to retain risk management consulting services. In conjunction with the consultants, the UW System is developing a materiality matrix. Materiality, for purposes of the pilot effort, is defined as the measurement of the relative impact or severity of a risk event on those areas that have significant value to the UW System. The materiality matrix has its foundation in the UW System’s annual Accountability Report. As the ERM process evolves, it is anticipated that a refined materiality matrix will give institutions a tool to more effectively measure, evaluate, and benchmark those issues that substantively characterize and impact the UW System. See Appendix C for a copy of the Materiality Matrix.

[25] CURIE Newsletter, Volume 14 Issue 3; September 2003; “University Risk Control Starts with Risk Assessment,” by Keith Shakespeare

The following are priority ranked ERM risks developed by two universities.[26]

University A		University B	
1.	Athletics	1.	Global Activities
2.	Critical Infrastructure	2.	Student Safety
3.	Data Security	3.	Data Security
4.	Emergencies and Crises	4.	Clinical Billing
5.	Employment Issues	5.	Environmental Pollution
6.	Financial Stewardship	6.	Human Subjects
7.	Health & Environment	7.	Post-Award Research
8.	Information Technology		
9.	Intellectual Property		
10.	International Programs		
11.	Patient Care		
12.	Public Safety and Security		
13.	Research Integrity and Assurance		
14	University Governance		

Might compiling a risk portfolio itself create risk? Some higher education attorneys may express concern that a risk portfolio could become evidence in a lawsuit and used against the institution in litigation. Take this example. A college includes deferred maintenance of facilities among its top priority risks. Several months later, a campus visitor trips on a broken stairway and suffers a serious injury. The visitor files a lawsuit. In pre-trial discovery, the visitor could obtain a copy of the priority risk list and pointedly question why the college had not fixed the stairway. This example involves litigation begun after the risk portfolio was created. Litigation already pending at the time the ERM process began raises similar issues.

Other higher education attorneys are comfortable with risk portfolios and priority risks. They accept that most adverse risks have a legal component but are not exclusively legal. Any risk treatment, they reason, may have legal consequences. They appreciate that resources are finite and believe that the institution's reasonable business judgments can be successfully defended. They are prepared to show

[26] University A is anonymous. University B is the University of Washington. Its February 2007 list appears at www.washington.edu/regents/meetings/minutes/2007/2feb.pdf

that the institution made decisions and took actions in good faith. Under this view, ERM is a positive step that can provide evidence of reasonable efforts to protect students, staff, and visitors.[27]

Here are some ideas to limit the potential legal vulnerability of risk lists and ERM processes:

Add a disclaimer to any risk portfolio or priority risk list explaining that the institution has limited resources and is working within them to address the identified priorities.

State priority risks as positive, best practice statements. Rather than “we need to fix the crumbling infrastructure,” say instead “we strive to have buildings that are maintained and safe for the building occupants.”

Consider limiting distribution of priority risk lists to those with a need-to-know. This will not shield the lists entirely from disclosure to adverse litigants, but it is prudent practice for any sensitive business information.

Consider appointing the general counsel to chair, or serve on, the ERM committee. He or she can structure the work and written materials to take advantage of available legal privileges.

Step 13: Assess your risks: validate and prioritize

After identifying the risks of greatest concern to the institution, those risks will need to be evaluated. Begin by assessing any existing risk management controls that apply to the priority risks. How well are current controls working? Also look to the wider context of existing risk management processes and compliance programs. Do existing policies and procedures apply to the priority risk and how effective are they? Another component of the assessment is the effective use of resources. Check whether the institution devotes appropriate resource levels to the priority area. If, for example, globalization is a strategic institutional initiative, are suitable resources allocated to eliminate unacceptable levels of uncertainty in international programs? Look also at compliance with applicable laws and regulations.

A validation workshop can be used to:

- Ensure accuracy in prioritization of risks
- Build support and buy-in to the process
- Assign risk ownership
- Establish acceptable mitigating techniques and agreements

Before convening a validation workshop, do the following:

- Give careful consideration to the selection of participants. Whom do you want to participate, why, and what can they bring to the discussion?
- Prepare the participants for active engagement by providing information in advance about what you hope to achieve from the workshop.
- Appoint a facilitator who can knowledgeably lead the discussion to get to the endpoint you hope to reach.
- Encourage validation workshop participants to look beyond their respective areas of expertise when considering ERM activities.

[27] Many of these concepts are drawn from the presentation on Emory University’s ERM process at www.treasuryinstitute.org/resourcelibrary/Symposium_2008/handouts/23.pdf.

An institution assesses a priority risks in light of its appetite for risk and tolerance of uncertainty.

The relationship between risk and reward is well known. As risk increases, so does the possibility of reward and loss. Simply, the less risky the opportunity, then the more limited the reward. COSO's ERM Framework defines risk appetite as "the amount of risk an entity is willing to accept in pursuit of value." Risk appetite applies to that which can and can not be measured quantitatively. An institution may quantify its appetite for endowment return risk. Its appetite for academic rigor, however, is generally more qualitative. A college or university's business and academic objectives, and strategy to achieve those objectives, help to define its risk appetite and the level of acceptable uncertainty.

When the pursuit of opportunities is managed well, the risk trade-off decreases and the return trade-off increases. This can lead to the pursuit of riskier opportunities in a continuation of achieving higher returns.

To help determine risk appetite, ask the following questions:

- What risks will the institution not accept? These might include academic quality compromises, regulatory compliance fines, and electronic data breaches.

- What risks will the college or university take with any new initiatives? Examples are lower than desired student registrations for a new academic program, and anticipated controversy over a new research project.

- What risks will the institution accept for competing objectives? An example of competing objectives might be a high volume of research grants versus fewer grants that present greater potential for technology transfer revenue.

COSO defines *risk tolerance* as the acceptable range of variation the entity is willing to accept in achieving its stated objectives. In the world of investing, risk tolerance is the range within which an investor can handle declines in the value of his/her portfolio. Risk tolerance helps establish acceptable boundaries around entrepreneurial behavior and the implementation process.

Risk tolerance will vary depending upon the risk. It is the point in which capital is no longer made available to absorb a loss or a particular activity. It identifies when the risk/reward trade-off decreases to a level at which the institution chooses to no longer absorb it. The degree to which compliance exposures are tolerated, for example, is often based on the amount of the potential fines associated with individual regulations.

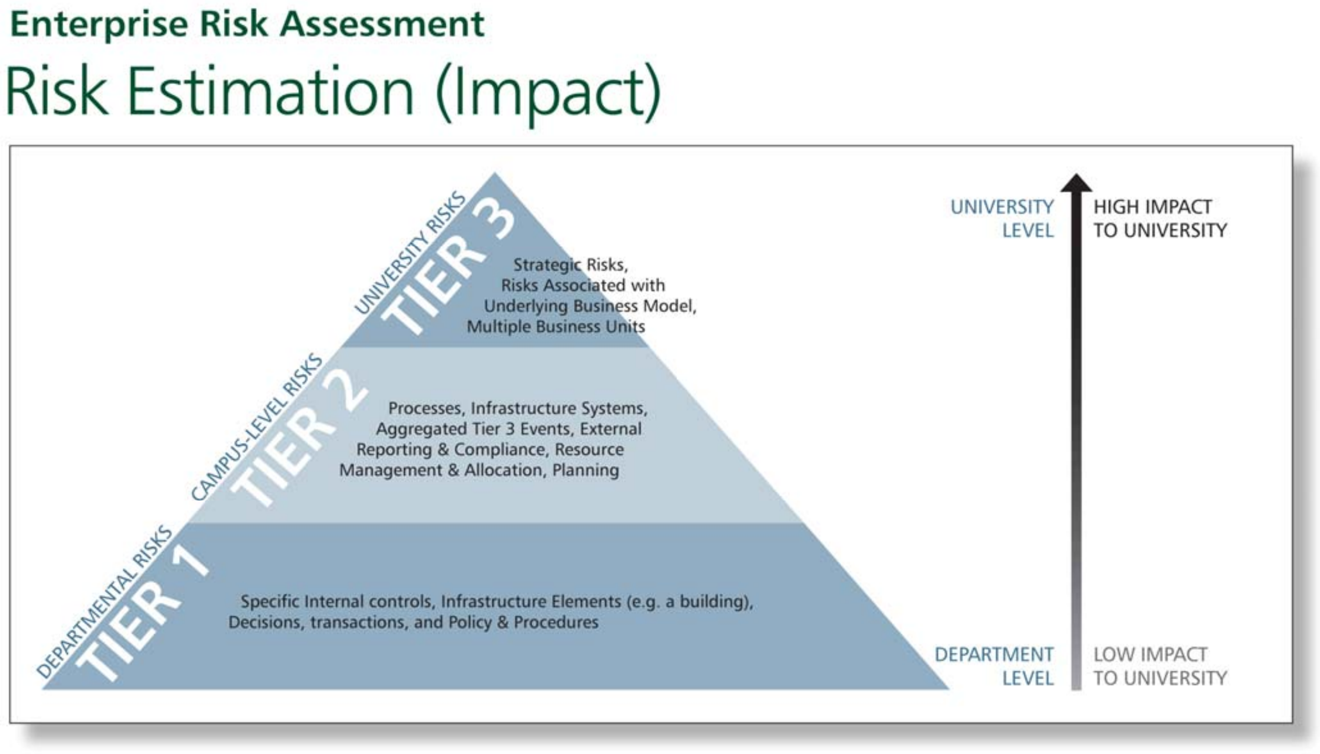
A Risk Council can provide tools to help individual employees assess risks as they make decisions.

The Maricopa County Community College District has developed two useful items. The "SMART" tool asks seven basic questions, has the user plot a risk map, and reminds the user of the District's vision, mission, and values. MCCCD has also developed a risk assessment "wallet card" that many MCCCD employees carry with their identification badges. Both tools are reprinted in Appendix B.

The University of Wisconsin System has provided a sample of their Risk Management Self-Assessment tool. See Appendix C.

Visual representations provide an easy way for readers to grasp the institution's main risks. Graphics can focus attention on the most significant risks and allow comparisons across different functions. Charts and graphs can quickly convey information to governing board members, senior leaders, and others. Traditional risk management graphic tools generally plot risk probability, impact, and cost to mitigate. A Risk Council may want to explore designing richer visual representations. Elements might include, among others, degree of uncertainty, benefits to the institution, total cost-of-risk, and financial value or impact.

Georgetown University has developed a pyramid to assist with the prioritization of risks. The pyramid has three tiers that correspond to the scope and impact of a particular risk. Broader risks are situated at the top of the pyramid and involve "university-level" risks that could affect the institution's strategic objectives or underlying business model. Risks in this category are considered high impact events that warrant the attention of the board and senior leadership. The middle of the pyramid corresponds to "campus-level" risks and includes risks associated with processes, infrastructure systems, and aggregated interdepartmental risks. "Departmental" risks are at the bottom of the pyramid and correspond to lower priority risks associated with specific internal controls, infrastructure elements, transactions, and policies and procedures.[28]


Enterprise Risk Assessment
Risk Estimation (Impact)
UNIVERSITY RISKS
TIER 3
Strategic Risks, Risks Associated with Underlying Business Model, Multiple Business Units
CAMPUS-LEVEL RISKS
TIER 2
Processes, Infrastructure Systems, Aggregated Tier 3 Events, External Reporting & Compliance, Resource Management & Allocation, Planning
DEPARTMENTAL RISKS
TIER 1
Specific Internal controls, Infrastructure Elements (e.g. a building), Decisions, transactions, and Policy & Procedures
UNIVERSITY LEVEL
HIGH IMPACT TO UNIVERSITY
DEPARTMENT LEVEL
LOW IMPACT TO UNIVERSITY

Every institution can design mapping and measurement tools for institutional or departmental risk assessments that best fit its ERM model. One method to define levels of risk and visualize the results of an enterprise risk assessment process is to use an enterprise risk calculator to identify the coordinates for each risk that can then be plotted on a heat map.

While there are numerous methods to calculate the probability and impact of an individual risk event, an enterprise risk calculator permits consistent methodology to establish the relative ratings of each identified risk. The formula provides for the ability to weight risk both before and after the

[28] Used with permission, the Risk Estimation (Impact) pyramid is courtesy of Georgetown University.

implementation of mitigations, controls, and procedures. With the coordinates from the enterprise risk calculator, you can map each risk on a heat map, which will provide a good two-dimensional view of risk and is an excellent tool for communicating the results of a risk assessment process to senior management.

Recent thinking on ERM suggests that the next generation of visual tools will communicate the interplay between departments and external events.

ISO will be publishing a companion standard on risk assessment titled ISO 31010 Risk management - Risk assessment techniques. It is anticipated that this standard will go into detail on the risk assessment process, including specific instructions on how to perform particular methods, the strengths and limitations of each and critical outcomes. A sampling of some of the risk assessment methods that will be discussed include checklists, brainstorming, Delphi technique, SWIFT (structured "What-if"), human reliability analysis (HRA), root cause analysis, scenario analysis, toxicological risk assessment, business impact analysis, fault tree analysis, event tree analysis, cause and consequence analysis, cause and effect analysis, Monte-Carlo analysis and Bayesian analysis.

The Canadian Standards Association is working on an Implementation Guide to ISO 31000. This publication is intended to provide guidance on implementing ISO 31000. Its application is not intended to be limited to Canadian operations. It provides an overview of Risk Management roles and requirements according to size of operations and model risk maturity criteria. It is expected that this guide will be published in late 2009.

Given the broad scope of operations within a university setting, risk managers will appreciate access to a broad range of analysis methods. To some extent, the enterprise risk calculator permits you to establish a composite weighted rating among departments and recognize external events.

As a word of caution, avoid overly complex graphic representations and reports. They may inhibit questions, dampen group involvement, and undercut the idea that risk management is part of every job and every decision.

For examples of risk calculator and heat map, see Appendix D.

Step 14: Assign ownership and take action

Once identification and evaluation have occurred, decisions will need to be made on how best to manage or treat the risks. Risk Council members may not have detailed knowledge about each priority risk. They should, instead, identify the people within the institution who work most closely within each risk area. If, for example, faculty recruitment is a major priority risk, one or more members of the ERM group should contact the people most responsible for faculty hiring in the program areas of concern.

Address the priority risks through the people with appropriate authority. This may, or may not, be the person most knowledgeable about the risk.

The committee can work with the identified “risk owners” to develop a plan to treat their risks. The usual options are:

1) Reduction: Reduce the likely frequency or severity of loss. You can, for example, change the way you conduct the activity or prepare better to handle problems should they occur.

2) Control: Minimize damage after a loss has occurred.

3) Transfer: Assign responsibility for performing a risky activity to another party. Indemnification provisions and insurance are forms of risk transfer.

4) Acceptance: Assume responsibility. After other steps have been taken to mitigate, control, and transfer the risk of an activity or operation, the institution may decide to accept any residual risk that remains. Consider instances where no treatment method is selected. That amounts, by default, to accepting risk.

5) Avoidance: Eliminate, or never launch, the activity because the risks appear too great.

A committee member can monitor the work of each functional expert. Risk Council members could allocate the monitoring function among themselves along lines such as these:

- Institution-wide Risks – Cabinet Member
- Operational Risks – Internal Audit
- Hazard Risks – Risk Manager
- Financial Risks – CFO

Try to delegate responsibility to an individual rather than a group, as accountability often gets fuzzy in groups. An individual more easily becomes the owner of the risk.

ERM from Plans to Action

At The Pennsylvania State University, an appointed committee launched the “ERM Key Initiative.” Committee members interviewed 55 administrators to develop an overall risk portfolio. The committee evaluated each risk to gauge its probability and likely impact. The group selected a small number of areas for initial review with the responsible departments. The committee is now monitoring the departments’ steps to address those risks. Some of the steps are new, while others existed before the ERM Key Initiative began.

The following Risk Matrix is drawn from a Heat Map guiding the treatment of priority risk areas.

Risk Priority Key
1= Minimum
2= Low
3= Medium
4= High
5= Maximum

Risk Name	Risk Level	Potential Impact	Risk Owner	*Current* Risk Treatment	*New* Risk Treatment	Next Review Date
Lack of Business Continuity Plans	Med/Low	Severe				
IT Security	Low	High				
Residence Hall Fire Safety	Low	High				
Tuition Default Rate	Med/Low	High				
Student Applicants	High	High				
Budget Rescissions	High	Maximum				
Attraction & Retention of Employees	Medium	Medium				
Inadequate Library Storage Conditions	High	Medium				

Strive to acquire suitable resources to address each priority risk. As one Think Tank participant said, “It’s useless to identify problems as priorities and then not allocate appropriate resources to them.”

Plans to treat the priority risks will involve some action steps. Resources will be needed to develop and implement any new policies, training, communication strategies, reminders, and other steps for the priority risk areas**.** Develop and implement plans as appropriate to the risk. Training was a common theme in the Think Tank discussion. A major goal of ERM is to give staff the tools and training they need to make their own decisions.

Given that resources are always finite, what level is appropriate? The best answer is an amount that is reasonable in light of the situation. Discussions of the materiality of the prioritized risks and their potential financial impacts are essential to resource requests.

Step	Phase Three: Implementation	Start Date	Target Finish
12	Develop a risk portfolio		
13	Assess your risks: Validate and prioritize		
14	Assign ownership and take action		

Phase Four: Sustaining Your ERM Program

The ERM process is never finished. As a process valuable to the entire institution, it should remain effective and sustained over time. Success often stimulates awareness of even greater possibilities that may be achieved if efforts are improved and professional expertise is strengthened.

The Risk Council will become the primary body to maintain the ERM process. It will continue to manage future risk identification and validation processes, oversee implementation of action steps, and make reports on continuation efforts.

Sustainability is dependent upon continuous improvement, otherwise the process becomes rote and stale, and interest and commitment begin to wane. Continued enhancement and improvement should be the goal of every ERM initiative.

The cycle of continuous improvement builds on success. In its simplest form, continuous improvement repeats the following steps, with new advancements in each repetition.

- Identify and measure the risk
- Define the goals and mitigation tasks
- Select risk owner(s)
- Agree on process
- Establish a measurement means
- Agree on time, personnel, and budget
- Establish milestones
- Report to Risk Council

At its most effective, ERM will allow an institution to become more aggressive in its ability to seize opportunities and succeed in achieving the results it seeks.

Step 15: Assess results

An important follow-up step for the Risk Council is to identify and monitor measures of performance of critical success factors. At an agreed-upon time after the first validation meeting and assignment of risk ownership, the Risk Council should convene and assess results. This allows the leadership team to revisit their previous work and look at whether the desired outcomes and specific goals have been achieved.

With increasing emphasis on accountability, it is important for the Risk Council to be able to provide evidence of the success and effectiveness of its work. The Risk Council should demonstrate benefits and measurable outcomes. Assessing progress against goals can support the continuation of ERM.

Ask:

- What did we do?
- What were the outcomes?
- How did we measure them?
- What are our lessons learned?

Build on small, quick successes. Particularly if the ERM program originated in the middle of the institution rather than at the top, it can be important to share news about initial successes. Even if a positive development seems small, such as a single change in a long-standing process, show how it can affect the institution's potential success in meeting its objectives. Create a series of small, quick successes, broadcast them, and build on them.

Step 16: Meet and report

In addition to repeating the cycle of risk identification, evaluation, mitigation and follow-up, sustainability can be enhanced with annual workshops to refresh the ERM process. Workshop participants review the priority risks previously established and identify and assess new priorities. From this, the Risk Council will compile the results and present a snapshot assessment to senior leaders in the form of an annual report. The annual report should review the Council's work and make recommendations on risk treatment initiatives for inclusion in the institution's budget and strategic planning cycle.

A basic ERM annual report outline includes:

1. Restatement of the ERM mission statement

2. Overview of the ERM organizational structure, including list of participating staff and faculty with their positions or roles on campus.

3. Overview of the year's major achievements and successes, for example, progress made on the past year's priority risks, and what, if any, activities the Risk Council organized and the outcomes of those activities.

4. A summary of those goals that were not attained and why

5. A summary of major on-going challenges

6. New goals for upcoming year

7. Summary of resource needs

Dashboard graphics are useful to include in the annual report to provide a quick understanding for the reader of the selected ERM performance measures. Dashboards include line graphs, bar graphs, pie charts, indicator lights, meters and gauges, and traffic signals. They are used to illustrate any variances from the established goals.

Annual reports are a means to demonstrate the Risk Council's achievements and the overall value of ERM to the institution.[29]

[29] For a copy of Maricopa Community Colleges' 2008 Annual ERM Report, go to http://www.maricopa.edu/mira/pdfdocs/annual_report08.pdf

Step 17: Review and realign risk treatment with available resources

Look occasionally at whether the steps selected for treating the priority risks are working and whether they remain adequate. Compare alignment with reality to ensure that the institution's resources are being used effectively to manage priority risks. Over time, risk treatment plans may require revision, whether upward or downward in scale. The risk owner needs to report regularly to the Risk Council on progress as well as challenges.

Check the adequacy of resources allocated to controlling priority risks**.** Are they sufficient and available on a continuing basis? If resources are needed, revise the strategies for treating the risks.

A review process might include:

- Revisiting the mission, priorities, risk owners, and the need for any additional support and/or resources
- Identifying what's working well and what needs adjusting
- Identifying how adjustments can be made and implementing the adjustments

Establish ways to measure progress and results. An important component of ERM is establishing quantitative and/or qualitative metrics and tracking them over time. The metrics may address total cost-of-risk, claims trends, or other numerical measures. Qualitative measures might include opinions about the impact of risks on the institution's progress in advancing its mission. One Think Tank participant suggested that assigning metrics to ERM in higher education may be more subtle than doing so in the corporate world. "In higher education, people aggressively take on risk. They may not actually see how much risk they are assuming." ERM metrics can help open their eyes to the upside and downside of the risks they take.

Whether the data is quantitative or qualitative, collect it in a timely fashion and provide reports to senior administration on recent progress.

Allocating Resources to Address a Priority Risk

One research university identified conflict of interest as a priority risk area. The ERM committee found that researchers regularly completed the proper forms for disclosure of potential conflicts. The staff position to review the forms and manage the process, however, had never been funded. The committee brought the problem to the attention of the higher-level ERM review committee, which promptly allocated money to fill the position.

Step 18: Do not neglect traditional risk management functions

Traditional risk management is a key component of an ERM initiative. Areas such as insurance purchasing, claims management and safety compliance need continual attention. Make sure that an ERM initiative does not usurp the time and attention that these functions require.

Step 19: Review any ERM framework you have selected to follow

As explained in Step 8, some campus ERM initiatives are modeled after a national or international standard, such as COSO or ISO, while others are not. If you modeled your program on a standard, occasionally review that standard. You will likely find new ideas and approaches to enhance your program. Even if your program is not modeled after a standard, compare your program to ones at other institutions and continue to learn. Standards, compliance issues, and ways to assure ERM effectiveness continue to evolve.

Step 20: Develop an institution-wide system for communicating

This step should occur concurrently with all the preceding steps.

Communicate widely and often. It is difficult to communicate too much about an ERM initiative. Spread news about an institution-wide launch in newsletters and emails. Tap your marketing staff for help in getting the word out and building enthusiasm. Seek internal publicity even for a small pilot project. Explain what ERM is, how the institution is starting to embrace it, and what it means to every employee. If feasible, include expressions of support from top administrators, board members, or other thought leaders on campus. Business schools often have faculty who teach ERM. They may appreciate the opportunity to contribute to the process to gain practical experience.

Encourage all staff members to become involved. Ideally they will become comfortable sharing information about not only successes but also close calls, disappointments, stalled results, and failures. Unfavorable information is important to assessing and managing movement toward institutional objectives. For some institutions creating the right non-punitive institutional culture can be challenging. Anonymous hot lines and policies against retaliation help. Tackle this issue in the context of your institution’s existing culture. All personnel need to feel safe in sharing adverse information.

Find opportunities to educate constituencies about how to factor the effect of uncertainty into the decisions they make.

As one Think Tank participant stated, their ERM process created a “risk nervous system” on campus. Everyone is committed to the process and is alert to risks and how to manage them.

Phase Four: Sustaining your ERM Process		Start Date	Target Finish
15	Assess results		
16	Meet and report		
17	Review and align risk treatment with available resources	Ongoing	Ongoing
18	Do not neglect traditional risk management functions		
19	Review any ERM framework you have selected to follow		At least annually
20	Develop an institution-wide system for communicating	Ongoing	Ongoing

Conclusion

Enterprise risk management is effective risk management. It allows institutions to fully benefit from the opportunities they seek. ERM's greatest attribute is that it is a good business practice. With it, an institution can better assure:

- A well protected reputation
- Success with opportunities
- Continuity of operations in the event of a catastrophe
- Overall improvement of institutional campus operations and campus life

But, effective ERM doesn't happen overnight. Sometimes enthusiasm alone for an ERM program can lead to a positive campus response and early implementation successes. On the other hand, in undertaking any new initiative, less-than-perfect results are common. Institutional culture may not be conducive to change, or people may be slow in acquiring new skills and knowledge.

Implementing ERM takes patience and persistence. As with any initiative, an institution can either delay while waiting for a perfect system or proceed and learn along the way. Success will rely on top level support, commitment of every person directly involved in the process, and the establishment of effective process and follow-through. Other success factors include:

- Clear ERM mission and goals
- Linage to all senior level planning and budget approval processes
- Sufficient resources
- Defined risk appetite and risk tolerance
- Assigned accountability
- Established risk aware culture with strong campus buy-in
- Continuous and sustained program

Sometimes even minor flaws may, unfortunately, lead to early abandonment of an otherwise rewarding ERM program. Pitfalls that can run the process off the road are:

- Lack of senior administration support
- Resistance to accountability
- Institutional inability to make a long-term commitment
- Inability to commit the required resources
- Difficulty in devising metrics
- Challenge of communicating with faculty and staff
- Unclear/unrealistic expectations
- Lack of clear mission and goals
- Poor planning

None of the pitfalls is insurmountable. Just be forewarned and prepared to address them.

Last, ERM is a process, not a guarantee. While no college or university can completely eliminate uncertainty, ERM provides the surest route forward.

Chart of the Complete Road Map

The following chart compiles the phases and steps of ERM implementation discussed in this report. Adapt the tasks and action items to fit your own situation. Although communication, reporting, and monitoring appear as the last step in the final phase, they should be performed throughout the entire process.

Step	Phase One: Building a Case for ERM	Start Date	Target Finish
1.	Understand the institution's plans, environment, and culture		
2.	Determine the status of your existing risk management processes		
3.	State your goals and objectives		
4.	Present the case		
5.	Obtain top-level commitment, support, and participation		
	Phase Two: Building an ERM Foundation	**Start Date**	**Target Finish**
6.	Name a project leader		
7.	Plan your project and incorporate a timeline		
8.	Select or design an ERM framework that best fits the institution's goals and campus culture		
9.	Create a cross-functional Risk Council		
10.	Create a mission and goals statement for the Risk Council		
11.	Develop a risk vocabulary and definitions		
	Phase Three: Implementation	**Start Date**	**Target Finish**
12.	Develop a risk portfolio		
13.	Assess your risks: validate and prioritize		
14.	Assign ownership and take action		
	Phase Four: Sustaining your ERM Process	**Start Date**	**Target Finish**
15.	Assess results		
16.	Review and realign risk treatments with available resources		
17.	Meet and Report		
18.	Do not neglect traditional risk management functions		
19.	Review any ERM framework you have followed		
20.	Develop an institution-wide systems for communicating	Ongoing	Ongoing

Selected Resources

“Developing a Strategy to Manage Enterprise-wide Risk in Higher Education” from NACUBO (2001)
www.nacubo.org/documents/business_topics/PWC_Enterprisewide_Risk_in_Higher_Educ_2003.pdf

Enterprise Risk Management Research from the North Carolina State University College of Management
http://mgt.ncsu.edu/erm/NCStateResearch.php

Enterprise Risk Management Resources from the Risk Management and Insurance Society
www.rims.org/ERM/Pages/default.aspx

“ERM in Higher Education” from URMIA (2007)
www.urmia.org/library/docs/reports/URMIA_ERM_White_Paper.pdf

“ERM: Rating Agencies Forcing the Issue” by Michael Moody, Rough Notes (March 2008)
http://findarticles.com/p/articles/mi_qa3615/is_200803/ai_n25139695/

Implementation Plan for Maricopa Integrated Risk Assessment Project at the Maricopa County Community College District Implementation Plan http://www.maricopa.edu/mira/pdfdocs/Impl_Plan.pdf

“Meeting the Challenges of Enterprise Risk Management in Higher Education” from NACUBO and AGB (2007)
www.nacubo.org/documents/business_topics/NACUBOriskmgmtWeb.pdf

“The State of Risk Management in Colleges and Universities Today” from AGB and United Educators (2009) www.agb.org/user-assets/documents/AGBUE_FINAL.pdf

Appendix A: Websites of Sample Campus ERM Programs

Maricopa County Community College District
Maricopa Integrated Risk Assessment (MIRA)
www.maricopa.edu/mira/index.php

Penn State University
www.fandb.psu.edu/risk/default.shtml

Texas A & M University
http://universityrisk.tamu.edu

University of California
www.ucop.edu/riskmgt/erm.html

University of North Carolina at Chapel Hill
http://finance.unc.edu/treasury--risk-management/risk-management/welcome.html

University of Washington
www.washington.edu/admin/finmgmt/erm

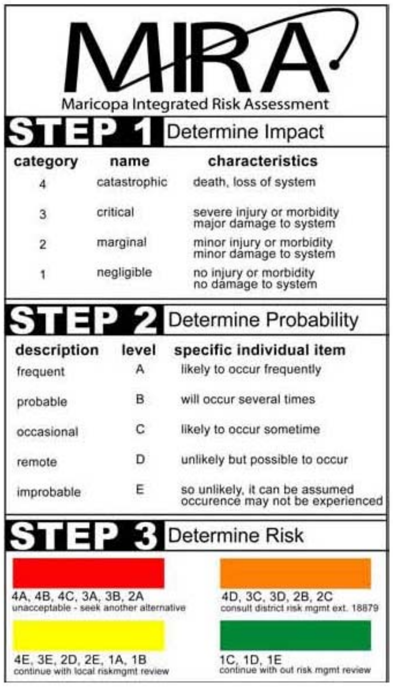
Appendix B: Measurement Tools and Reporting Processes

A useful article is “Enterprise Risk Management: Tools for Self-Assessment,” by Andrew Faris, March 2008, University of Washington. It is available at http://f2.washington.edu/treasury/riskmgmt/sites/default/files/ERM%20Tools%20for%20Self%20Assessment.pdf

Also, see the “Sample Risk Assessments by Campus Experts” in the Appendix of the AGB/UE report. To access a copy, visit www.agb.org/user-assets/documents/AGBUE_FINAL.pdf.

The Maricopa County Community College District has developed two useful risk assessment tools. One is called the SMART Tool, with SMART standing for “Strategic Maricopa Assessment Risk Tool.” The other is a wallet card given to each employee and usually carried with his or her identification badge. Both appear in the following pages.[30]

Wallet Card



MIRA

Maricopa Integrated Risk Assessment

STEP 1 Determine Impact

category	name	characteristics
4	catastrophic	death, loss of system
3	critical	severe injury or morbidity major damage to system
2	marginal	minor injury or morbidity minor damage to system
1	negligible	no injury or morbidity no damage to system

STEP 2 Determine Probability

description	level	specific individual item
frequent	A	likely to occur frequently
probable	B	will occur several times
occasional	C	likely to occur sometime
remote	D	unlikely but possible to occur
improbable	E	so unlikely, it can be assumed occurence may not be experienced

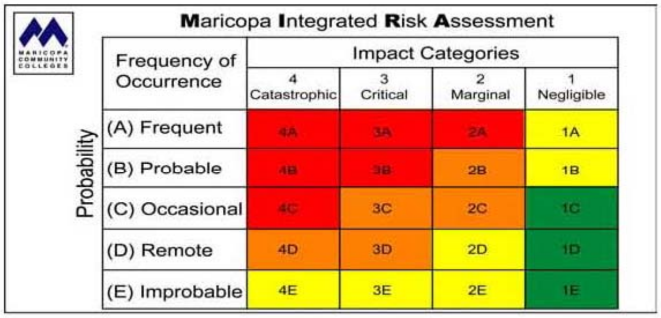
STEP 3 Determine Risk

🟥 4A, 4B, 4C, 3A, 3B, 2A
unacceptable - seek another alternative

🟧 4D, 3C, 3D, 2B, 2C
consult district risk mgmt ext. 18879

🟨 4E, 3E, 2D, 2E, 1A, 1B
continue with local riskmgmt review

🟩 1C, 1D, 1E
continue with out risk mgmt review



Maricopa Integrated Risk Assessment

	Frequency of Occurrence	Impact Categories			
		4 Catastrophic	3 Critical	2 Marginal	1 Negligible
Probability	(A) Frequent	4A	3A	2A	1A
	(B) Probable	4B	3B	2B	1B
	(C) Occasional	4C	3C	2C	1C
	(D) Remote	4D	3D	2D	1D
	(E) Improbable	4E	3E	2E	1E

[30] Used with permission, the SMART wallet card, and the following SMART tool and MIRA risk map are courtesy of the Maricopa County Community College District.

MIRA

Maricopa Integrated Risk Assessment

A New Way of Looking at Risk

SMART

Strategic Maricopa Assessment Risk Tool

A Simple Model for Self-Assessing Risks To Achieving Objectives

Risk Assessment Activity or Project:
Date Risk Assessment Conducted:
Risk Assessment Group Members:

This tool is based on risk being defined as "The opportunities, uncertainties, threats, or barriers to which MCCCD must respond in order to achieve its objectives."

1. Review MCCCD's Vision, Mission & Values Statements.

2. List your department's objectives.

3. List the opportunities of the proposed activity or program.

4. List the risks that can prevent you from achieving your department's objectives for the proposed activity or program.

5. Using the Risk Map, assess the probability and impact of each risk.
   a. What is the probability of this risk occurring considering what you are doing today to prevent it?
   b. What is the impact on your ability to achieve its objectives if this risk occurred?

6. Starting with your highest risk, answer the following questions for each of your five highest risks?

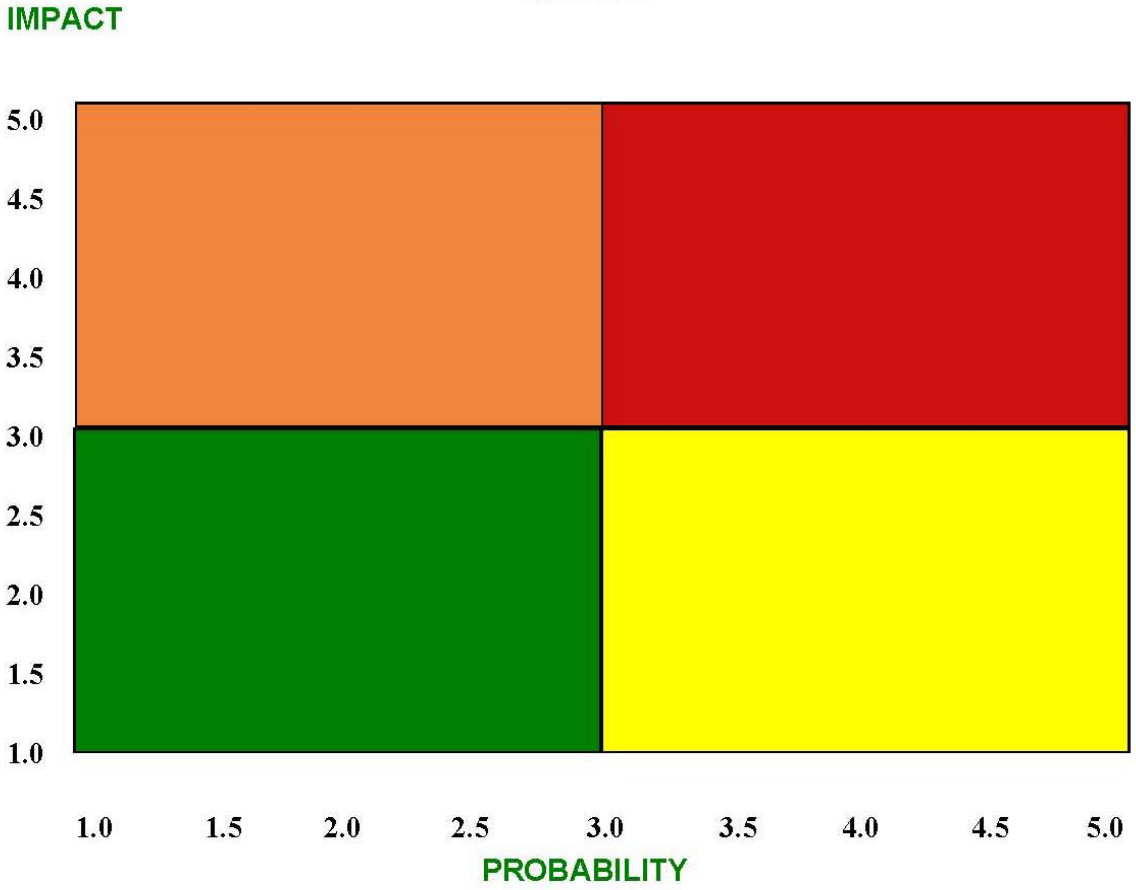
   a. What are we doing now to prevent this risk or reduce its impact?
   b. Is what we are doing effective in preventing this risk or reducing its impact to a level we consider acceptable?
   c. What else should we do to prevent this risk or reduce its impact to a level we consider acceptable?
   d. Who else do we need to work or consult with to prevent this risk or reduce its impact to an acceptable level?

7. Do we move forward with this activity or program?

MIRA

Maricopa Integrated Risk Assessment

RISK MAP



Appendix C: Risk Management Self-Assessment[31]

This self-assessment is intended to assist you in asking critical questions about risk awareness and to initiate a broader discussion on risk preparedness. Risk can be defined as any issue or event that impacts an organization's or unit's ability to meet its objectives. You are encouraged to think of the financial, operational, compliance, strategic, or reputational risks that your unit faces.

1) Have key risks and vulnerabilities associated with your unit's responsibilities or objectives been identified? Examples could include cash handling, compliance with federal or state requirements, or inventory controls.

2) Does your unit have a process for identifying or assessing risk? If so, what criteria are used to identify risk? Examples include program complexity or growth, staff turnover, external scrutiny, or the quality of existing internal controls.

3) Has your unit evaluated specific risks based on frequency or impact?

4) Do you believe risks have been adequately identified and communicated to senior management?

5) What risk mitigation methods are currently used by your unit? Examples include insurance or internal controls.

6) Are you aware of risks outside of your unit that may have an impact on your unit's objectives? Examples may include network security and records confidentiality.

7) Have there been recent major changes to your area of responsibility or control such as new federal regulations or organizational changes?

8) Have risks associated with recent changes been identified or assessed?

Questionnaire Instructions

This questionnaire is intended to help UW System Administration identify a broad range of risks related to each area's goals and objectives. Risk can be defined as any issue or event, including missed opportunities, that impacts the ability to achieve stated objectives or defined goals.

To help organize your response and provide a framework for further analysis we have identified five risk categories – financial, operational, compliance, strategic, and reputational. We have added sub-categories, as well, to exemplify common areas of activity within each category. Feel free to add any new sub-categories as needed to best describe the risks being identified within each category. The categories and sub-categories are shown below:

- Financial: Revenues, Expenditures, Cash Management, Trust Funds/Fixed Assets;
- Operational: Human Resources, Auxiliaries, Information Systems, Physical Plant/Facilities, Academic
- and Student Services;

[31] Used with permission, all items in Appendix C are courtesy of the University of Wisconsin System.

- Compliance: Environmental & Occupational Safety, Athletics, Privacy, Records Management;
- Strategic: Access, Diversity, Budget; and
- Reputational: Ethics, Fraud, and Academic Standards/Accreditation.

Identify risks by program area within each category for your area of responsibility or knowledge. The program area is simply a description of where the risk is present within the organization.

Specify a risk factor. A risk factor is a description of why the risk exists. Examples may include transaction volume or amount, program complexity or changes, or reduced resources. Please be as specific as possible.

Lastly, assign a rating value between 1 and 5 for two risk attributes – impact and probability, for each identified risk. Use your best judgment and the tables below, when assigning values. Intermediate ratings (ratings not listed) can be used to refine your response.

Impact		
Very High	5	Loss would call into question viability of the institution/system
Medium	3	Loss would disrupt operations or threaten the viability of a single business process
Very Low	1	Loss is within acceptable or reasonable range associated with day-to-day activities
Probability		
Very High	5	Loss is likely to occur on a day-to-day basis.
Medium	3	Loss is likely to occur within the upcoming year.
Very Low	1	Occurrence of a loss in the near term is possible, but unlikely.

Examples of factors you may want to consider when assigning impact and probability values include: the financial amount or activity; length of time since the last internal or external review; the level of program complexity; the use or handling of confidential data or information; staff turnover; and the presence of internal controls or risk management efforts.

UW SYSTEM UNIT		
PREPARED BY		DATE:

RISK CATEGORY	RISK SUB-CATEGORY		IMPACT	PROBABILITY RATING
	PROGRAM AREA	RISK FACTOR	RATING	
Financial	Expenditures			
	Example: Purchasing Cards	High transaction volume	2	4.5
	Revenues			
	Cash Management			
	Trust Funds/Fixed Assets			
	Other			

UW SYSTEM UNIT		
PREPARED BY		DATE:

RISK CATEGORY	RISK SUB-CATEGORY		IMPACT	PROBABILITY RATING
	PROGRAM AREA	RISK FACTOR	RATING	
Compliance	Environmental & Occupational Safety			
	Athletics			
	Privacy			
	Open Records & Records Management			
	Other			

UW SYSTEM UNIT		
PREPARED BY		DATE:

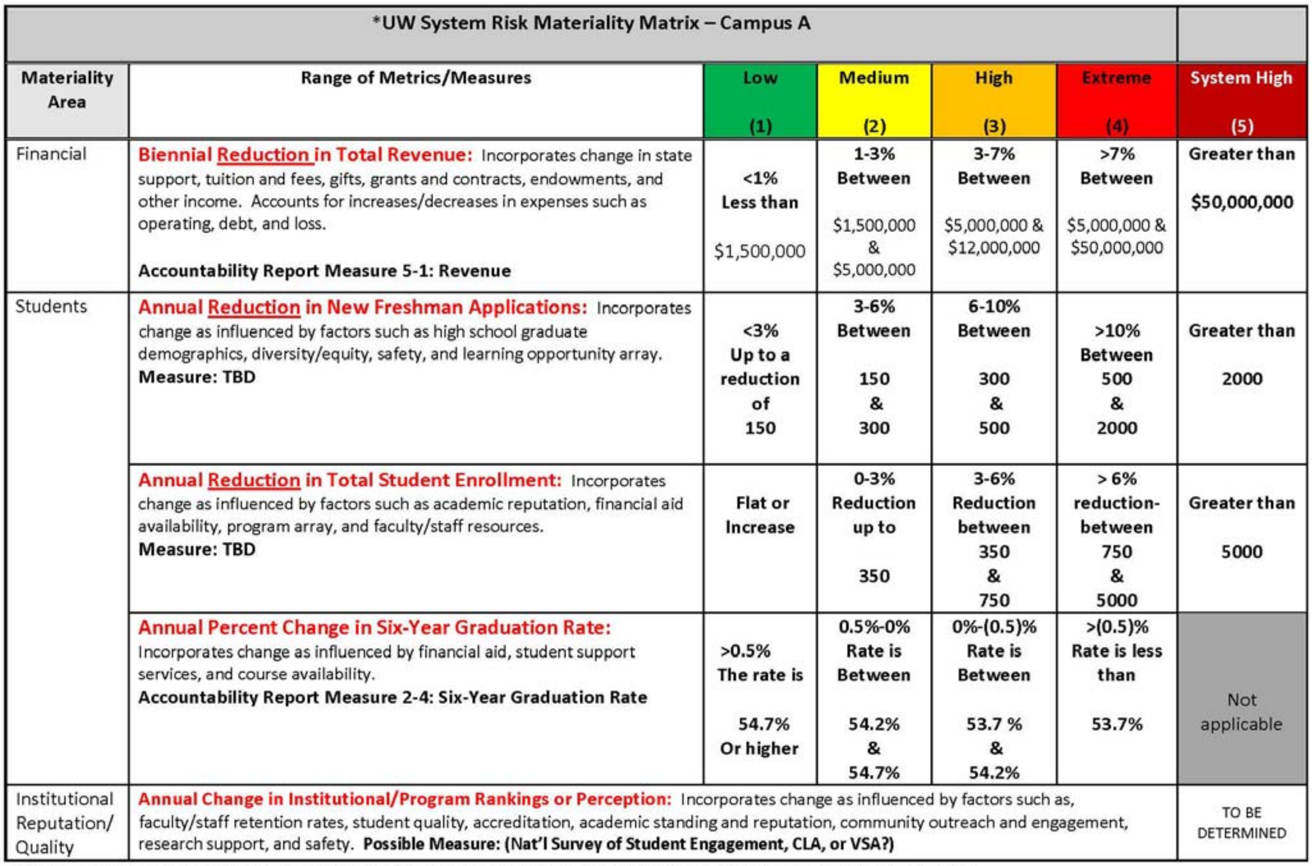
RISK CATEGORY	RISK SUB-CATEGORY		IMPACT	PROBABILITY RATING
	PROGRAM AREA	RISK FACTOR	RATING	
Operational	Human Resources			
	Auxiliaries			
	Information Systems			
	Physical Plant/Facilities			
	Academic Services			
	Student Services			
	Other			

UW SYSTEM UNIT		
PREPARED BY		DATE:

RISK CATEGORY	RISK SUB-CATEGORY		IMPACT	PROBABILITY RATING
	PROGRAM AREA	RISK FACTOR	RATING	
Strategic	Access			
	Diversity			
	Budget			
	Other			

UW SYSTEM UNIT		
PREPARED BY		DATE:

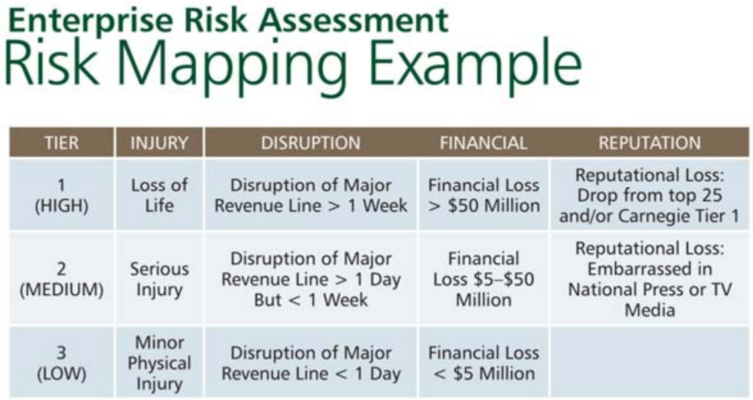
RISK CATEGORY	RISK SUB-CATEGORY		IMPACT	PROBABILITY RATING
	PROGRAM AREA	RISK FACTOR	RATING	
Reputational	Ethics			
	Academic Standards/Accreditation			
	Fraud			
	Other			



*UW System Risk Materiality Matrix – Campus A						
Materiality Area	**Range of Metrics/Measures**	**Low** **(1)**	**Medium** **(2)**	**High** **(3)**	**Extreme** **(4)**	**System High** **(5)**
Financial	**Biennial Reduction in Total Revenue:** Incorporates change in state support, tuition and fees, gifts, grants and contracts, endowments, and other income. Accounts for increases/decreases in expenses such as operating, debt, and loss. **Accountability Report Measure 5-1: Revenue**	**<1%** **Less than** $1,500,000	**1-3%** **Between** $1,500,000 & $5,000,000	**3-7%** **Between** $5,000,000 & $12,000,000	**>7%** **Between** $5,000,000 & $50,000,000	**Greater than** **$50,000,000**
Students	**Annual Reduction in New Freshman Applications:** Incorporates change as influenced by factors such as high school graduate demographics, diversity/equity, safety, and learning opportunity array. **Measure: TBD**	**<3%** **Up to a** **reduction** **of** **150**	**3-6%** **Between** **150** **&** **300**	**6-10%** **Between** **300** **&** **500**	**>10%** **Between** **500** **&** **2000**	**Greater than** **2000**
	Annual Reduction in Total Student Enrollment: Incorporates change as influenced by factors such as academic reputation, financial aid availability, program array, and faculty/staff resources. **Measure: TBD**	**Flat or** **Increase**	**0-3%** **Reduction** **up to** **350**	**3-6%** **Reduction** **between** **350** **&** **750**	**> 6%** **reduction-** **between** **750** **&** **5000**	**Greater than** **5000**
	Annual Percent Change in Six-Year Graduation Rate: Incorporates change as influenced by financial aid, student support services, and course availability. **Accountability Report Measure 2-4: Six-Year Graduation Rate**	**>0.5%** **The rate is** **54.7%** **Or higher**	**0.5%-0%** **Rate is** **Between** **54.2%** **&** **54.7%**	**0%-(0.5)%** **Rate is** **Between** **53.7 %** **&** **54.2%**	**>(0.5)%** **Rate is less** **than** **53.7%**	Not applicable
Institutional Reputation/ Quality	**Annual Change in Institutional/Program Rankings or Perception:** Incorporates change as influenced by factors such as, faculty/staff retention rates, student quality, accreditation, academic standing and reputation, community outreach and engagement, research support, and safety. **Possible Measure: (Nat'l Survey of Student Engagement, CLA, or VSA?)**					TO BE DETERMINED

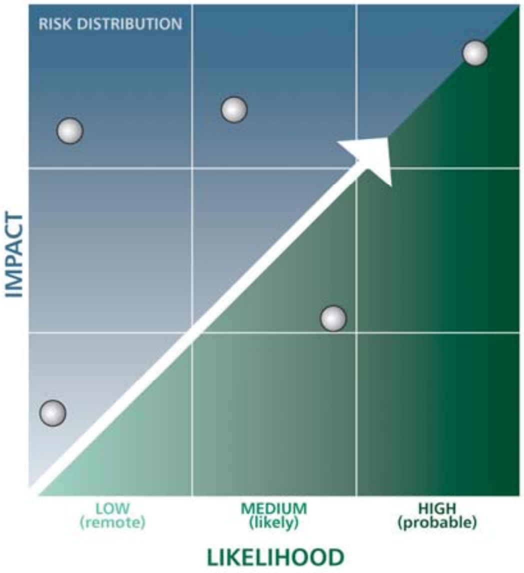
*Developed in conjunction with Core Risks Ltd/Shelter Island Risk Services, a Division of Gallagher Bassett Services, Inc.

Appendix D: Risk and Heat Map Examples[32]



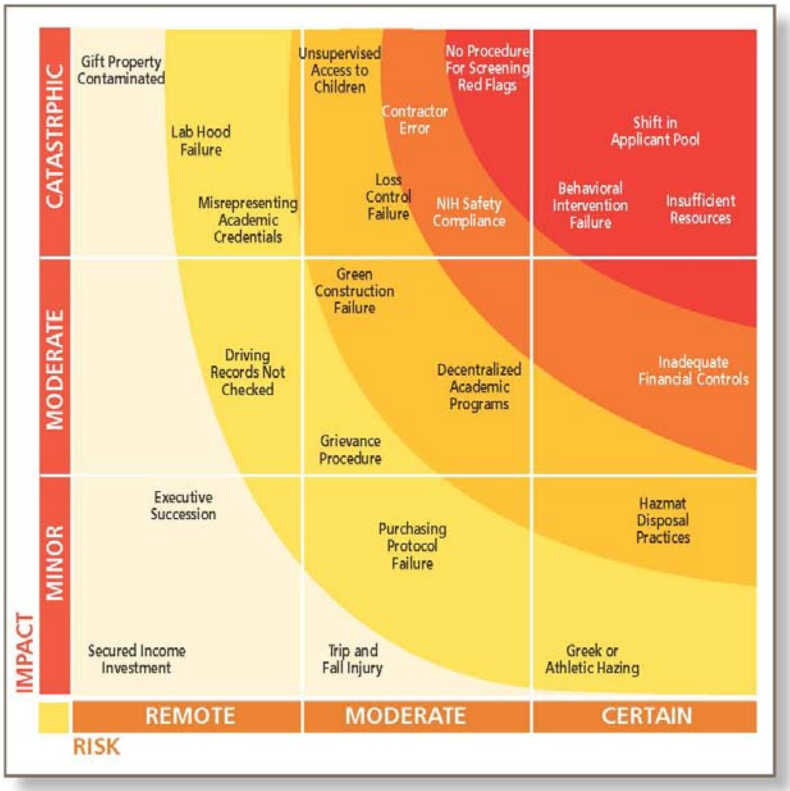
Enterprise Risk Assessment
Risk Mapping Example

TIER	INJURY	DISRUPTION	FINANCIAL	REPUTATION
1 (HIGH)	Loss of Life	Disruption of Major Revenue Line > 1 Week	Financial Loss > $50 Million	Reputational Loss: Drop from top 25 and/or Carnegie Tier 1
2 (MEDIUM)	Serious Injury	Disruption of Major Revenue Line > 1 Day But < 1 Week	Financial Loss $5–$50 Million	Reputational Loss: Embarrassed in National Press or TV Media
3 (LOW)	Minor Physical Injury	Disruption of Major Revenue Line < 1 Day	Financial Loss < $5 Million	



[32] Used with permission, the Risk Map Example is courtesy of Georgetown University.

SAMPLE
Heat Map



Gift property contaminated: after receipt, an unknown underground hazardous chemical plum is discovered encroaching on the property.

Executive succession: no plan in place when untimely departure of Provost results in disruption to new academic program and lost opportunity to recruit a nationally recognized research team.

Secured Income investment: fails to earn any income for multiple years.

Trip and fall injury: resulting from debris on steps at stadium is proximate cause of a broken arm. The student's medical insurer subrogates to the institution for reimbursement. The student requests accommodations for all classes for balance of semester.

Lab hood failure: due to deferred maintenance, an exhaust fan fails, resulting in exposure to contaminants that lead to acute and chronic health effects for those exposed.

Misrepresenting academic credentials: confirmation of credentials not part of the recruiting and hiring process. Discovered after professor is granted tenure; leads to revocation of tenure in highly publicized media reports.

Driving records not checked: for employees that operate vehicles routinely in scope of employment. Disclosed when institution van driver is determined to be at fault in collision with fatalities.

Grievance procedure: not followed by institution during a denial of tenure appeal; results in ongoing distractions as tenure committee members are required to respond to time-consuming depositions.

Purchasing protocol failure: in multiple major transactions results in being routinely overbilled for ongoing services.

Greek or athletic hazing: goes unrecognized by the institution until a non-sanctioned off-campus hazing incident results in life threatening injuries to 3 students; highly sensationalized by media since perpetrator recorded the incident on cell phone and posted video to YouTube.

Unsupervised access to children: where no background checks of employees to determine if they are a registered sex offender.

Loss control failure: extended inaction by institution to insurance carrier mandatory loss control recommendations results in mid-term cancelation of insurance. Replacement coverage secured at more than twice the expiring premium.

Green construction failure: previously untested conservation practice fails to return sufficient savings to justify increased initial capital cost and actually results in increased ongoing operating cost of new facility.

Decentralized academic programs: results in common missteps resulting in faculty turnover and inability to observe and control grade inflation.

Hazmat disposal practices: EPA investigation determines the contracted disposal carrier illegally dumped computers and used batteries in landfill resulting in fines and closer review of all institutional hazmat practices.

Contractor error: Lack of safety program on renovation project results in multiple injuries and illnesses to students, faculty, staff, plus employees of contractor and sub-contractors. In addition to lawsuits, OSHA initiates aggressive review of institution's safety program.

NIH safety compliance: insufficient safety compliance regarding biosafety and animals leads to funding loss.

Inadequate financial controls: in Donor Services, leads to employee embezzlement that result in negative media coverage, tarnished reputation and rescinding of pledges.

No procedure for screening red-flags: in hiring process, results in offers of employment to individuals with negative information in their background check reports that should have resulted in no offer of employment. The terminated employees sue for wrongful termination.

Shift in applicant pool: of students goes unrecognized; resulting in decreased freshman classes for multiple years.

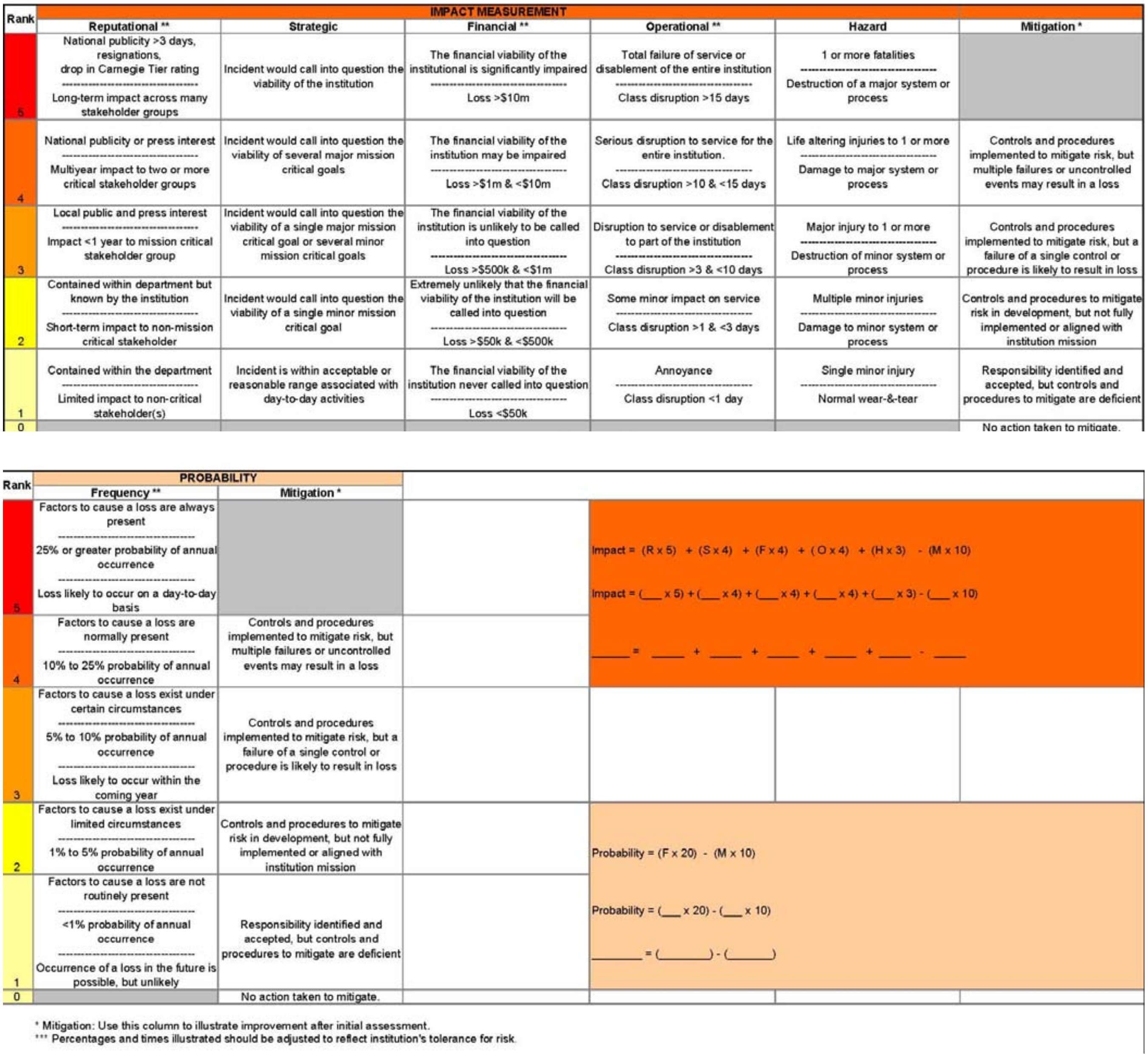
Behavioral intervention failure: due to inadequate awareness, the faculty and staff fail to report their observations of an at risk student, resulting in team's inability to apply risk rubrics to classify the potential threat. With no intervention, student violently strikes out injuring multiple individuals.

Insufficient resources: to provide comprehensive oversight of workplace and research risks and practices hinders research enterprise and ability to anticipate risks to employees and students, resulting in short- and/or long-term safety/health hazards, injury, illness, or death.

* The curves are illustrative and not representative of any particular formula. Each institution will need to establish their own risk tolerance thresholds for the various levels.

* The x and y coordinates for each example are based on assumptions and could shift significantly based on factors present in your own environment.

Appendix E: ERM Risk Calculator



Rank	IMPACT MEASUREMENT					
	Reputational **	Strategic	Financial **	Operational **	Hazard	Mitigation *
5	National publicity >3 days, resignations, drop in Carnegie Tier rating ----------------------------------- Long-term impact across many stakeholder groups	Incident would call into question the viability of the institution	The financial viability of the institutional is significantly impaired ----------------------------------- Loss >$10m	Total failure of service or disablement of the entire institution ----------------------------------- Class disruption >15 days	1 or more fatalities ----------------------------------- Destruction of a major system or process	
4	National publicity or press interest ----------------------------------- Multiyear impact to two or more critical stakeholder groups	Incident would call into question the viability of several major mission critical goals	The financial viability of the institution may be impaired ----------------------------------- Loss >$1m & <$10m	Serious disruption to service for the entire institution. ----------------------------------- Class disruption >10 & <15 days	Life altering injuries to 1 or more ----------------------------------- Damage to major system or process	Controls and procedures implemented to mitigate risk, but multiple failures or uncontrolled events may result in a loss
3	Local public and press interest ----------------------------------- Impact <1 year to mission critical stakeholder group	Incident would call into question the viability of a single major mission critical goal or several minor mission critical goals	The financial viability of the institution is unlikely to be called into question ----------------------------------- Loss >$500k & <$1m	Disruption to service or disablement to part of the institution ----------------------------------- Class disruption >3 & <10 days	Major injury to 1 or more ----------------------------------- Destruction of minor system or process	Controls and procedures implemented to mitigate risk, but a failure of a single control or procedure is likely to result in loss
2	Contained within department but known by the institution ----------------------------------- Short-term impact to non-mission critical stakeholder	Incident would call into question the viability of a single minor mission critical goal	Extremely unlikely that the financial viability of the institution will be called into question ----------------------------------- Loss >$50k & <$500k	Some minor impact on service ----------------------------------- Class disruption >1 & <3 days	Multiple minor injuries ----------------------------------- Damage to minor system or process	Controls and procedures to mitigate risk in development, but not fully implemented or aligned with institution mission
1	Contained within the department ----------------------------------- Limited impact to non-critical stakeholder(s)	Incident is within acceptable or reasonable range associated with day-to-day activities	The financial viability of the institution never called into question ----------------------------------- Loss <$50k	Annoyance ----------------------------------- Class disruption <1 day	Single minor injury ----------------------------------- Normal wear-&-tear	Responsibility identified and accepted, but controls and procedures to mitigate are deficient
0						No action taken to mitigate.

Rank	PROBABILITY			
	Frequency **	Mitigation *		

5	Factors to cause a loss are always present
	----------------------------------- 	
	25% or greater probability of annual occurrence
	----------------------------------- 	
	Loss likely to occur on a day-to-day basis
				Impact = (R x 5) + (S x 4) + (F x 4) + (O x 4) + (H x 3) - (M x 10)
				Impact = (___ x 5) + (___ x 4) + (___ x 4) + (___ x 4) + (___ x 3) - (___ x 10)

4	Factors to cause a loss are normally present ----------------------------------- 10% to 25% probability of annual occurrence	Controls and procedures implemented to mitigate risk, but multiple failures or uncontrolled events may result in a loss		_____ = _____ + _____ + _____ + _____ + _____ - _____
3	Factors to cause a loss exist under certain circumstances ----------------------------------- 5% to 10% probability of annual occurrence ----------------------------------- Loss likely to occur within the coming year	Controls and procedures implemented to mitigate risk, but a failure of a single control or procedure is likely to result in loss		
2	Factors to cause a loss exist under limited circumstances ----------------------------------- 1% to 5% probability of annual occurrence	Controls and procedures to mitigate risk in development, but not fully implemented or aligned with institution mission		Probability = (F x 20) - (M x 10)

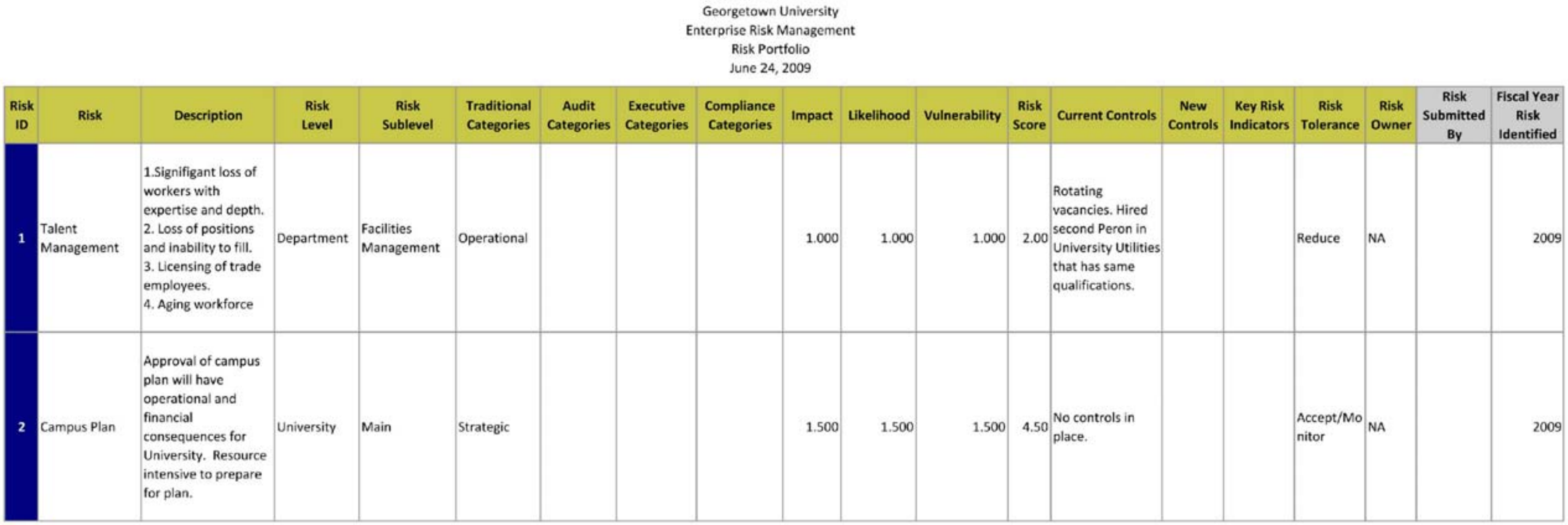
1	Factors to cause a loss are not routinely present
	----------------------------------- 	
	<1% probability of annual occurrence
	----------------------------------- 	
	Occurrence of a loss in the future is possible, but unlikely
		Responsibility identified and accepted, but controls and procedures to mitigate are deficient		Probability = (___ x 20) - (___ x 10)
				________ = (________) - (_______)

0		No action taken to mitigate.		

* Mitigation: Use this column to illustrate improvement after initial assessment.

*** Percentages and times illustrated should be adjusted to reflect institution's tolerance for risk.

Appendix F: Risk Matrix[33]



Georgetown University
Enterprise Risk Management
Risk Portfolio
June 24, 2009

Risk ID	Risk	Description	Risk Level	Risk Sublevel	Traditional Categories	Audit Categories	Executive Categories	Compliance Categories	Impact	Likelihood	Vulnerability	Risk Score	Current Controls	New Controls	Key Risk Indicators	Risk Tolerance	Risk Owner	Risk Submitted By	Fiscal Year Risk Identified
1	Talent Management	1.Signifigant loss of workers with expertise and depth. 2. Loss of positions and inability to fill. 3. Licensing of trade employees. 4. Aging workforce	Department	Facilities Management	Operational				1.000	1.000	1.000	2.00	Rotating vacancies. Hired second Peron in University Utilities that has same qualifications.			Reduce	NA		2009
2	Campus Plan	Approval of campus plan will have operational and financial consequences for University. Resource intensive to prepare for plan.	University	Main	Strategic				1.500	1.500	1.500	4.50	No controls in place.			Accept/Monitor	NA		2009

[33] Used with permission, the Risk Matrix is courtesy of Georgetown University.

Appendix G: Definitions of Common Terms Used with ERM[34]

Audit Department Risk Assessment
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 as a *"high risk department"* does not necessarily mean that it 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

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

[34] Used with permission courtesy of the Maricopa County Community College District.

Purpose of ERM

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

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

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
An institution’s tolerance for risk. The broad amount of risk a college or university is willing to accept in pursuit of its mission or vision.

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

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 tortuous 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. "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 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 be 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 probability and/or impact (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.

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

Traditional Risk Management
Original form of risk management focusing primarily on insurable hazard risks.