June 2023

URMIA Enterprise Risk Management Resource for Higher Education

UNIVERSITY RISK MANAGEMENT & INSURANCE ASSOCIATION

HIGHER EDUCATION RISK MANAGEMENT

Contributors

Kate Cosgrove Booth, PhD
Assistant Vice President Risk & Compliance, Northwestern University

Courtney Davis Curtis, CPCU, ARM, ARM-E
Assistant Vice President for Risk Management and Resilience Planning, University of Chicago

Carrie Frandsen, MBA, ARM-E, RIMS-CRMP
Systemwide Enterprise Risk Management Director - Office of the President, University of California

Saumya Khanduja, CIA
Assistant Director – Institutional Risk Management, Massachusetts Institute of Technology

Christine Packard
Assistant Vice President for Enterprise Risk Management, University of Massachusetts

Ellen Shew Holland, DRM, ARM, MSF
President, Strategic Risk Frameworks

Lisanne Sison
Managing Director, ERM and ESG, Gallagher

Fitzroy Smith, CPCU, ARM
Assistant Vice President, Compliance, Safety & Enterprise Risk Management, American University

Tim Wiseman, MBA, ARM-E, CDFM-A (Ret.)
Chief Risk Officer, University of Wyoming

Editors

Rachel Kuper
URMIA Learning Specialist

Gary Langsdale, DRM, ARM
URMIA Education Manager (Ret.); Assistant Vice President & University Risk Officer, The Pennsylvania State University (Ret.)

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

UNIVERSITY RISK MANAGEMENT & INSURANCE ASSOCIATION

HIGHER EDUCATION RISK MANAGEMENT

Contents

A. Executive Summary

This document outlines the importance of having an enterprise risk management (ERM) program in higher education and provides guidance as to why it is an asset to an institution and how it can be conducted in an effective manner. Given higher education's broad scope of activities and challenges, it is important that institutions and boards provide their students, faculty, staff, and alumni with a level of certainty that risks and opportunities are identified, assessed, and managed appropriately. Through having a better awareness of the issues that can impact the achievement of the institution's strategic goals, an entity can address these issues in an effective and integrated manner to support the achievement of objectives.

In this document we will provide:

- A discussion of the origins of ERM.
- The benefits of having a program in support of your strategic goals.
- An overview of frameworks and references for guidance.

The Association of Governing Boards (AGB) annually provides a "Top 5 Strategic Risks" list, and a recent version includes "managing serious risks." Post-Covid-19 they are seeing that:

- Institutions will need to be better prepared to manage these risks in the future.
- None of the major risks cited in its 2020 list were resolved several years later, and it is important to manage the key risks and continue moving forward while shoring up the framework to manage other significant risks.

This document will provide you and your team with a better understanding of how to implement a strategic ERM program utilizing various levels of resources while allowing you to embed risk mitigation and focus on the goals ahead.

B. Introduction

Organizations face inherent risk in all their activities. ERM is a systematic way to manage such risk more effectively. ERM assists organizations in making informed decisions about their objectives, the level of risk they are willing to assume, and the controls required to support achieving their objectives. However, risk management and internal control are not objectives by themselves; they are an integral part of setting and achieving the organization's objectives. The goal of ERM is to mature risk management in the organization and enhance the organization’s risk culture so that risk management becomes a business enabler of strategic value to the organization. Ideally, ERM becomes invisible when risk is managed as an integral part of managing the organization. This corresponds with the main objective of an organization, which is not to effectively manage risk or to have effective controls, but to ensure that it makes the best decisions and achieves its objectives.

First, a few definitions as a guide:

- Governance- The set of responsibilities and practices exercised by the governing body with the goal of providing strategic direction; ensuring that objectives are achieved; ascertaining that risks are managed appropriately; and verifying that the organization’s resources are used responsibly. The governing body and subsequent levels of management integrate governance into strategy, management, oversight, and accountability to achieve sustainable organizational success.
- Risk Management- Coordinated activities to direct and control an organization with regard to risk.
- Risk Management Framework- A set of components that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization.

- Risk Management Process- The systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk.
- ERM Principles:
    - Risk management should be integrated into all aspects of the organization's operations, from strategic planning to daily decision-making.
    - Risk management should be a collaborative effort that involves all levels of the organization from the board of directors to front-line employees.
    - Risk management should be based on a sound understanding of the organization's risks and exposures.
    - Risk management should be flexible and adaptable to the ever-changing business environment.

By following these principles, organizations can improve their ability to identify, assess, and manage risks. This can help them make better decisions, achieve their objectives, and lessen the likelihood of adverse surprises.

ERM is not a new concept, either in the for-profit and nonprofit business worlds or within higher education's unique governance model. ERM has evolved from the practice of risk management and is increasingly being recognized as a best practice, as risk management professionals continue to embrace a portfolio of traditional risks while also considering a broader, holistic view of all types of risks that could impact the higher education institution. As the field of risk management has become more strategic, so has the strategy associated with assessing and managing the broad spectrum of risks within higher education entities. In 2000, the National Association of College and University Business Officers (NACUBO), in consultation with the accounting firm PwC, published a document outlining a potential strategy to embrace the ERM concept within the higher education governance framework based on, but not strictly following, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework for Internal Controls.

At about that same time, several leading universities initially took up the process of looking more broadly at risks, some spurred by Congress enacting the Sarbanes-Oxley Act in response to several significant accounting scandals, and the concept began to spread (albeit slowly within higher education). By 2007, URMIA had published its own white paper, *ERM in Higher Education*, which is still relevant and available today in the URMIA Library - including four case studies that contrast varying approaches to developing an ERM program. Gradually, other schools began to explore the concept, and by 2014 and the publication by AGB of Janice Abraham's *An Accountability Guide for University and College Boards*, AGB's poll showed that up to 35% of schools were in some stage of developing an ERM program.

By the book's second edition in 2020, data showed that the adoption of ERM had grown, but was still in place at fewer than 50% of polled colleges and universities. However, during the Covid-19 pandemic, institutional leaders and their governing boards were forced to confront previously unimaginable operational, strategic, and existential risks. This led to significant new interest in the concept of ERM and, in some cases, increased demands upon risk managers at institutions who found themselves overwhelmed with "opportunities" for identifying, quantifying, and prioritizing strategic and operational risks across the institution. It was at this point that URMIA recognized the need for more up-to-date material that would be useful to its members as they worked to manage risks in the broader sense.

This new resource is intended to provide resources for those interested in starting – or continuing – an ERM program at their institution. Although logically organized, it is not designed to necessarily be read front-to-back. Rather, it is a collection of resources that will each add to one's understanding of ERM and provide insights into ERM program development.

URMIA wishes to thank each of the contributors - all leaders in the field; their time and talent were freely and generously given and have enabled us to provide a guide that URMIA members will find worthwhile.

C. What Is Enterprise Risk Management (ERM)?

The typical definition of ERM usually includes statements along the line that “ERM is a framework for managing organizational risk.” That is probably the preamble to the ERM definition of some five years ago; however, as ERM has evolved, the new focus of ERM is to help leaders increase the likelihood of meeting organizational objectives, rather than simply compiling a list of potential issues.

The Covid-19 pandemic made it abundantly clear that universities have no choice but to plan for the unexpected. The number, complexity, and inter-connectedness of the major pandemic-driven risks underscore the need for institutions of higher education (IHE) to have an agile, flexible, and data-driven ERM process.

Let’s start by defining risk. A common definition is that risk is an event, situation, issue, or change in circumstances which adversely impacts the IHE’s ability to meet its goals and objectives. Therefore, an IHE must understand and determine its risk appetite (which is the level of risk-taking a university is willing to accept) while pursuing its objectives and opportunities before action is taken to mitigate the risk.

ERM takes a holistic approach to managing risks. Individuals, teams, and business units still manage the risks in their area of responsibility, and they are supported by strong networking, communication, and reporting mechanisms that enable people to communicate and manage risks at the speed of the business. ERM establishes a systematic process of monitoring, identifying, analyzing, evaluating, managing, and fostering strategic actions that address the uncertainties that present risks to the achievement of the organization’s objectives, including opportunities to gain a competitive advantage.

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

A strong ERM program sets the tone for the culture at the IHE and is dynamic in that it focuses on identifying emerging risks and on detecting changes to existing risks and the effectiveness of policies and processes to manage those ongoing risks. A proactive ERM program manages an organization's current risks while monitoring and preparing for emerging risks. A static and siloed approach to ERM tends to slow the program down and reduces the linkages to decision-making by senior or executive leadership that would otherwise reinforce a resilient institution. As the IHE matures in ERM, it is the emerging risks that may be assessed to determine and understand the impact of such risks over time. As the pace of change continues to escalate, it is becoming more apparent that institutions need to make decisions more rapidly and flexibly. This means that being able to detect risk and determine the appropriate action in real time is needed to remain resilient to disruption and to maintain a competitive advantage.

IHEs are experiencing many transformational changes that impact their ability to achieve financial and academic success. The "emerging risks" of just five to ten years ago are here to stay. These include declining student enrollments due to changing demographics and interests, financial instability, deferred maintenance, inflation, digital transformation, grade inflation, and the impact of reputational risk upon higher education. The "speed of technology" and its impact on the technology industry training its own employees faster and in a more focused manner than perceived in higher education is one example of such risks.

There are also many opportunities such as public/private partnerships where institutions can be a part of training current employees in addition to educating students for future careers in emerging industries. We also live in a far more globally connected environment than when URMIA first provided ERM observations in 2007. With this in mind, the regulatory climate has become more strict while global relations have struggled in several parts of the world. Given increased programs involving international travel and research, the risk and reputation of higher education continue to be a focus and require a strong lens in managing.

An effective ERM program provides senior-level executives and other stakeholders with a view into risks that may not be seen from the eye of the auditor or board member. Developing an effective ERM approach can be accomplished incrementally in accordance with the institution's objectives and strategic goals, risk culture, and resources.

Customizing an ERM program to match your entity's available resources and tailoring it to your strategic goals are key to meeting many of the challenges inherent in sustaining ERM. Key items to consider include:

- Having a core group that is streamlined, and not meeting just for the sake of having meetings. There must be a purpose. It is important to note that these programs can be conducted with a small, yet facilitated team versus by one person. Too many good risk managers have become "line managers" by trying to take on the management of all risks instead of facilitating for the risk owners.
- Trying to do too much at once which can be overcome by choosing to focus on a few risks to start. It's best to not let perfect be the downfall of good enough as risks are dynamic and change rapidly.
- Trying to "add layers or another silo" in a time of dwindling resources. This, too, can be overcome by using a focus on embedding your metrics into existing processes to improve them, as well as having the line manager hold the accountability for the success of their risk issues as outlined in the first item above.

D. Why Enterprise Risk Management?

ERM provides a holistic approach to risk mitigation benefiting the institution at large. A well-implemented program engages stakeholders at all levels of the organization, creating a uniform language and standardized approach for the optimization of risks. This is important because risks generally are viewed as negative, however, when managed appropriately, risks can positively generate opportunities. Because of this, an ERM program can ultimately provide strategic value and help an institution fulfill its mission.

ERM enables institutions to:

- Harmonize risk-related functions (e.g., audit, compliance, risk, etc.).
- Assign roles and responsibilities related to risk owners or supporting committee structures, establishing a risk accountability framework within the organization.
- Assess risk by way of scoring that takes into consideration remediation efforts allowing an institution to prioritize risks, determine the best treatment of risks, and better allocate resources.
- Evaluate risks objectively in a concise and consistent fashion especially where resources are limited.
- Enhance the timeliness of risk identification and remediation across the institution.
- Refine reporting to boards and senior leadership.
- Improve lines of defense with risk/processes, risk programs/functions, and independent assurance (e.g., auditors and regulators).
- Build confidence in risk governance serving as a solution for external parties who may inquire about such processes (e.g., insurers, debt assessors or rating agencies, and auditors).

There are benefits and opportunities in having a strong, effective, and well-oiled ERM program:

- The university is more nimble and better prepared to respond.
- Decisions can be made more quickly.
- Surprises are typically kept to a minimum due to the “forward-looking” nature of emerging risks.
- An integrated approach is taken which minimizes operating in silos.

E. Building an ERM Framework

Building an ERM Framework
Organizations often have some form of risk management in place, as employees naturally consider potential risks and opportunities when making decisions. However, this approach may not be comprehensive, coherent, consistent, or communicated effectively. A risk management framework is a set of principles, processes, and tools that help organizations identify, assess, and manage risks. It provides a systematic approach to risk management that can be tailored to the specific needs of the organization. To ensure effective and integrated risk management, organizations should employ a properly formed risk management framework as an integral part of their system of management. This framework should contain the necessary elements, be appropriate for the organization, and work effectively. By doing so, organizations can ensure that risk is managed at all times to create the maximum net benefit.

An ERM framework helps establish a consistent risk management culture that is grounded in the context of that specific institution. It is not dependent upon a single champion but articulates the who, why, and how of the organization's ERM efforts. An ERM framework organizes and aligns various risk management functions and helps entities manage complexity, visualize risk, assign ownership, and define responsibility for assessing and monitoring risk treatments on an ongoing basis.

Here are the key elements of a risk management framework:

- Governance- The framework should define the roles and responsibilities for risk management within the organization.
- Culture- The framework should promote a culture of risk awareness and accountability throughout the organization.
- Processes- The framework should define the processes for identifying, assessing, and managing risks.
- Resources- The framework should provide tools and resources to help organizations implement risk management processes.

The risk management framework should be integrated into all aspects of the organization's operations from strategic planning to daily decision-making. It should be a collaborative effort that involves all levels of the organization from the board of directors to front-line employees.

An ERM framework provides the rationale of why the organization has an ERM program and the overall goals and desired outcomes. Implementing an ERM program requires consistency, collaboration, and commitment, so taking the time to articulate the value proposition upfront - and ensuring everyone is on the same page and on board - is essential.

Below we have provided a common outline for an ERM framework that can function as a starting point for your institution's ERM efforts:

Desired Goals and Outcomes
This section describes your "pitch" for ERM at the organization and explains how this process will create and protect value for the organization. Common desired outcomes for ERM include effective allocation of resources; risk-informed decisions; an improved decision-making process; a reduction in losses/uncertainty; improved compliance; and improved resiliency/adaptability.

Leadership Commitment and Support
Use this section to describe where the authority for implementing ERM is coming from, whether it is coming from the board of trustees or your president/chancellor. This section is used to articulate that this is a key priority for the organization which has visibility and support at the highest levels of the institution.

Context
Organizations have different operations, organizational structures, and cultures so the ERM program needs to be tailored to fit each institution. A program structure designed for a large university system would not likely be a good fit for a small private liberal arts college. Defining the context should include reviewing the scope of operations at the institution, considering its internal and external environment, and evaluating the impact (if any) of the organization's structure and culture on its ability to effectively manage uncertainty. It may be helpful to use this section to connect to the organization's mission, strategy, and goals, which helps frame the role of ERM within the specific goals of the institution.

Roles and Responsibilities

Identify your key stakeholders and take the time to define their roles, responsibilities, and how they interact with each other. This is where you define your organization's risk governance structure. For example, who is responsible for providing periodic reports on risk management activities to the board of trustees? Is it the president or the chief risk officer? Where will they get the information they will present? What is the role of the ERM committee? What is the role of internal audit? What does the review and approval process for the organization's risk register look like? All of this should be evaluated and defined for the organization before the risk assessment is conducted.

Key Definitions

Like most advanced business practices, ERM can have a tendency to use a lot of jargon or to use common words in a certain way that benefit from clear and concise definitions to give context. In addition to defining the terminology an organization uses, the key definitions should also articulate what risk data the organization will collect (i.e., the information they will collect and maintain in their risk register), and what risk criteria they will use (impact, likelihood, velocity, recoverability, etc.).

ERM Process

The framework should provide a high-level overview of the schedule and process for the ERM program. The process articulated in the framework doesn't need to be incredibly detailed, but it should identify key deadlines and decision points. Typically, it takes about six to eight weeks to develop, finalize and approve an ERM framework, then another two to six months to implement the plan articulated in that framework and to conduct an inaugural risk assessment. The rest of the time is spent focusing on implementing mitigations and establishing a regular risk monitoring and reporting cadence.

Reporting

The framework should identify the frequency and content of reporting on the institution’s ERM activities. For example, an institution may decide to provide updates to the senior leadership team on a quarterly basis and provide an annual report to the board of trustees (or a committee of the board of trustees). It should be determined whether the updates will report on the process broadly or focus on the top five to ten risks that have been hand-selected for increased visibility, accountability, and ownership. Finally, the format of the reporting should also be determined, e.g., a formal annual report, a presentation, a dashboard, or a mix of various media.

Continuous Improvement

Lastly, the institution should consider when in their process they will review and identify opportunities to continuously improve their ERM activities. This should be a regularly occurring activity, whether it is scheduled on a periodic basis or built into regular ERM meetings.

Overall, the framework acts as a roadmap and can facilitate effective communication and ownership of ERM activities across the organization. A framework grounded in the best practices articulated in a standard (or in a combination of the standards) is one of the best tools to support a successful ERM journey.

F. Managing Expectations About the Results of an ERM Program

ERM is a multi-faceted resource for IHEs, but the responsibilities associated with ERM programs can often be misunderstood by leadership and risk partners alike. ERM is often confused with risk ownership and expertise in subject matter risks when, in fact, ERM leaders can be the "great facilitators" within your institution, responsible for bringing together disparate partners and rallying them around the common goal of reducing risk and maximizing opportunities.

To avoid confusion and appropriately set expectations for ERM within your institution, it is important to articulate the “Yes, It Does” and the “No, It Does Not” statements of your ERM program. Examples of these types of statements include:

Yes, It Does Statements

- Our ERM program facilitates a process to identify and assess the impact of risk on our institution.
- Our ERM program increases transparency on risk exposure.
- Our ERM program validates our institution’s capacity to mitigate risk.
- Our ERM program supports the development of a risk-informed culture.
- Our ERM program collaborates with risk partners and risk owners across the institution on risk.
- Our ERM program strategizes with leadership and risk partners on risk management.
- Our ERM program amplifies the responsibility of everyone at the institution as having a role in risk management.

No, It Does Not Statements

- Our ERM program does not own risk.
- Our ERM program does not implement risk mitigation strategies.
- Our ERM program does not manage compliance activities.
- Our ERM program does not audit risk mitigation activities.

These attributes of your ERM program should be communicated clearly and concisely using plain, straightforward language. The attributes should be stated often and consistently, particularly at the beginning of any presentation, meeting, or discussion about your ERM program.

G. Aligning the ERM Process with the Institution's Strategic Plans and Initiatives

One of the most impactful aspects of ERM is that it is designed to align an organization's risk management (and risk-taking) activities with its overall strategy, goals, and objectives. The way ERM can support the successful achievement of strategy can take form in two different, but related, ways.

Use ERM to Evaluate Strategy

The first way ERM can support strategy is through its use of analyzing the institution's initiatives and identifying potential challenges or barriers to the strategy that needs to be effectively managed for it to be successful. This also includes identifying opportunities that need to be exploited. For example, let's say that your institution has established an objective to diversify both the faculty and student body. ERM can be used to:

- Analyze the Goal/Objective – Ensure that the goal is stated clearly and that it includes the motivation or justification of why the goal is important to the institution. Ideally, the desired outcome should be clear, and the institutional leaders across the organization should have a shared understanding of why the goal is a priority.
- Evaluate the Context – Analyze the current environment to identify both internal and external contextual factors that contribute to the current state of the risk. Internal contextual factors can include things like organizational structure, current policies and procedures, existing leadership structure and composition, etc. External factors can include things like the diversity of the existing candidate pool, social and political pressure, geographic location of the institution, economic factors, etc.
- Identify Realities and Barriers – Once the institution understands both the justification for the goal and the current environment, it will be well-positioned to identify realities, barriers, threats, and opportunities, also known as risk identification.

- Prioritize – Once the risks related to the goal have been identified, they can then be prioritized in terms of which risks have the greatest potential to prevent the successful achievement of the desired goal or outcome.
- Treat – Once the high-priority threats have been identified, treatment strategies can be developed, evaluated, and implemented.

The outcome of this process is a roadmap that helps the organization anticipate challenges they may face as they work to execute their strategy and implement proactive management methods to support their success.

Use ERM to Set Strategy

The second method for using ERM to support the institution's strategy is to leverage the school's existing risk profile/portfolio to determine or advise what the institution's strategy should be. For example, let's say that the institution has identified risks related to an inability to recruit students with a particular educational profile or that potential students have different expectations that are not aligned with current institutional activities potentially impacting enrollment.

Assuming these risks are identified as "critical" to the organization, the activities undertaken to mitigate these risks represent a strategic imperative that must be addressed. Changes the institution implements to address these risks may fundamentally change its identity, curriculum, or learning environment, thus representing a shift in strategy. It will generally require a coordinated effort across multiple divisions of the institution to address. ERM can provide the framework and infrastructure for that coordination.

Such an approach allows an organization to respond to its risk profile in a strategic and coordinated way, and also create a loop where risks can inform strategy, and strategy can inform risk-aware action. It is this mechanism that will allow organizations that have implemented ERM to adapt to emerging risks more quickly and methodically.

ERM and Emerging Risks

As we all know, the risk environment is dynamic. This is not exclusive to the higher education industry; however, the impacts of emerging risks can be more diversified in a higher education setting than they may be in other sectors. For example, all organizations have been under increasing pressure to define and mobilize a strategy around environmental, social, and governance (ESG), however, this pressure manifests in higher education more in terms of reputational exposure than the board/investor pressure that publicly traded companies experience.

The increased scrutiny around ESG risks has created a shift in priority for many risks that were already known to institutions, but are now receiving additional scrutiny and interest from a broader group of stakeholders. For example, most institutions had risks related to diversity, equity, and inclusion (DEI), employee retention, or student enrollment on their risk register, but the shift in context has changed the overall priority of these risks, requiring a re-assessment and the development of a strategic approach to managing effectively.

Though ESG is a hot topic now, it is nearly a guarantee that the focus will be something different in five years. No matter what the environment holds, ERM can position organizations to adapt their strategy effectively and manage risks proactively.

H. Key ERM Tools and Processes

When considering ERM and its implementation or application, it is important to differentiate between an ERM framework versus an ERM process. The framework is the skeleton or structure within which the processes function. ERM processes are the actions and activities occurring within the framework. One of the most familiar ERM processes is that of risk identification, but this is just one of several processes and activities in the overall practice of ERM within the framework. Other processes include communication and reporting, sensing and gathering/refreshing risk information, and working with contributing ERM partners like counsel, campus safety, and internal audit. Management of the ERM processes can be challenging as actions and activities may occur simultaneously and involve numerous inputs from diverse business units, colleges, and departments. Given that staffing for facilitating ERM coordination at many institutions can be generally austere at best, it is important to leverage and integrate tools and other resources that support ERM efforts.

Some tools and resources ERM practitioners have found to be invaluable include:

Risk Management Information Systems (RMISs)	Heat maps
Document templates from ERM training workshops	Risk assessment techniques (ISO References)
Materials and references available at the North Carolina State University ERM initiative website/portal	URMIA, PRIMA, ACUA, NACUBO, IRM, NACUA, AFERM, AICPA, RIMS and other professional associations
Input-Process-Output or Lines of Operation models	Risk/finance/accounting consultants
Previously established auditing or compliance dashboards	Broker or insurance carrier training materials

A simple ERM process and framework, consistently applied, tunes the culture of the organization to the appropriate level of risk-taking and guides stakeholders toward covering risks at an enterprise level.

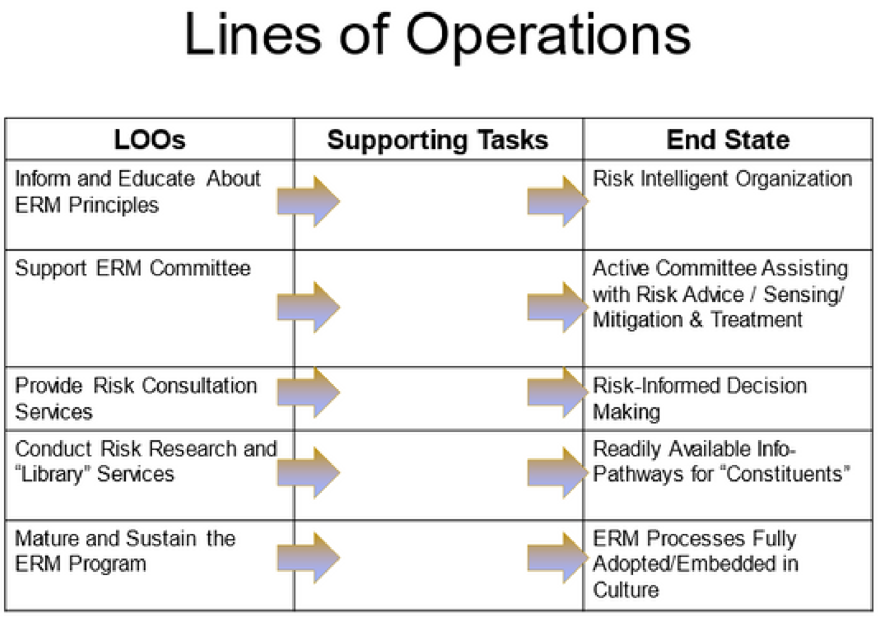
It is important to establish a common risk language that improves the understanding of risk and opportunity, consolidates risk information across the breadth of the institution, and is easily understood across all levels of the institution. This includes definitions of common terms used, a risk universe that provides a common set of risk categories and definitions, and baseline criteria for impact, likelihood, and any other factor (e.g., velocity, management preparedness) that the organization may choose to use to determine risk potential and/or exposure.

Risk universe and criteria documents used by higher education peers may be leveraged and customized to the needs and objectives of your organization. The URMIA Risk Inventory provides a broad list of risks that are common to colleges and universities. Using a subset of risks from this compilation that are relevant to your institution is a good foundation for early enterprise risk identification discussions.

Make easy-to-use templates such as those for risk mapping, scoring, prioritization, and assessments available to the community. These, too, can be resourced from peer networks and tweaked to fit your process and framework.

Once a business case has been built, an ERM program has been approved by institutional leadership, and stakeholders have been engaged, mapping the main processes and activities of an ERM program can help provide discipline and assist in keeping focused. One tool, for example, is a lines of operation table to identify key ERM essential processes or activities, the end-state or goal for them, and the intermediate activities or sub-processes required to get there. Working with an ERM steering group or an ERM committee to populate a lines of operation table also helps unify effort and establish a clear vision of what the process goals are and how tasks and activities fit into the larger ERM picture.

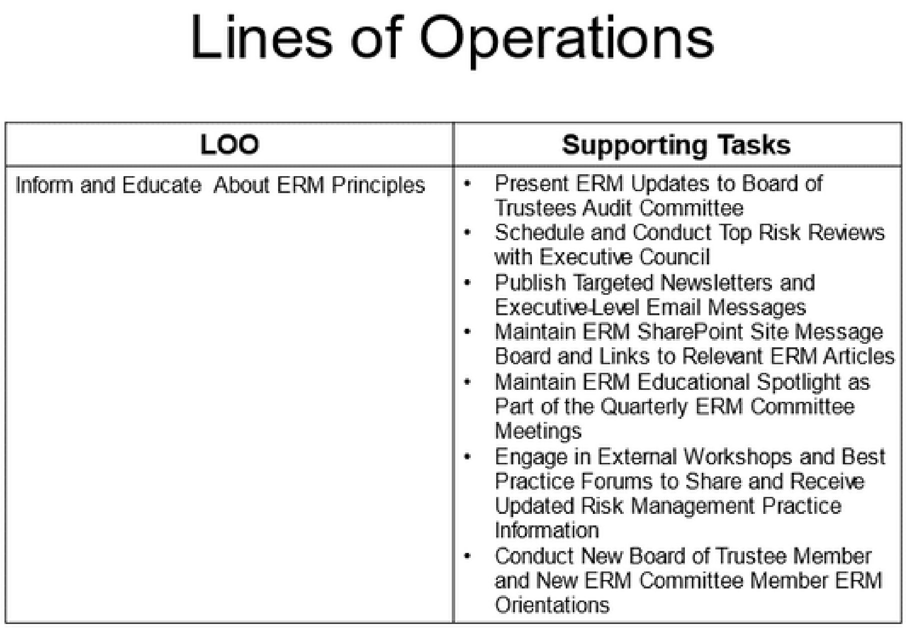
Basic Lines of Operation (LOO) Table Example



Lines of Operations

LOOs	Supporting Tasks	End State
Inform and Educate About ERM Principles		Risk Intelligent Organization
Support ERM Committee		Active Committee Assisting with Risk Advice / Sensing/ Mitigation & Treatment
Provide Risk Consultation Services		Risk-Informed Decision Making
Conduct Risk Research and "Library" Services		Readily Available Info-Pathways for "Constituents"
Mature and Sustain the ERM Program		ERM Processes Fully Adopted/Embedded in Culture

Example of Supporting Task "Build-Out" for One of the LOOs



Lines of Operations

LOO	Supporting Tasks
Inform and Educate About ERM Principles	• Present ERM Updates to Board of Trustees Audit Committee • Schedule and Conduct Top Risk Reviews with Executive Council • Publish Targeted Newsletters and Executive-Level Email Messages • Maintain ERM SharePoint Site Message Board and Links to Relevant ERM Articles • Maintain ERM Educational Spotlight as Part of the Quarterly ERM Committee Meetings • Engage in External Workshops and Best Practice Forums to Share and Receive Updated Risk Management Practice Information • Conduct New Board of Trustee Member and New ERM Committee Member ERM Orientations

The basic ERM process can be somewhat intuitive and not unduly complicated, although the practice of its elements can be more complex. While ERM is, by design, at some institutions a “top-down” approach to managing larger enterprise-wide risks in the strategic context, at other institutions it is operated “bottom-up” or “managed from the middle.” In any case, it is important to not overlook some very practical benefits and applications at the operational level. Since formal ERM processes help put risks in relevant perspective, this can lead to better stewardship and improved risk-informed (as opposed to emotion-driven) decision-making. It is helpful to sometimes ask, *“If ERM is the answer, what are the questions?”*

The following two vignettes are examples of how ERM outputs can assist in some real, tangible ways.

- The “Small Voice” of Import/Export Controls and Conflicts of Interest Reporting - Lisa Closewatch had recently been hired by the research division of Crowsnest University to serve as the university’s primary staff person overseeing the annual requirement for researchers and administrators to report any conflicts of interest with projects they are involved with at the university. She and an assistant are also involved in educating the university researchers on regulations related to imports and exports (and their controls) and ensuring compliance with related federal laws. Lisa seldom has the platform to bring concerns in either of her areas to the attention of senior leadership and because most of the university isn’t directly affected by either of her areas of responsibility, she is frequently frustrated and feels like the dust speck on the clover flower in *Horton Hears a Who.* She wonders, “Is there some process or venue that would help her get appropriate attention for her risk and compliance areas which, if not tended to, can lead to significant negative reputational, financial, and compliance consequences for the entire institution?”
- Trustee Procurement Card Concern - David Paycheck has been the chief financial officer for more than five years at Crowsnest University. He has had a good relationship with leadership and internal audit, but every time the Board of Trustees Audit Committee meets, regardless of the agenda or reports given, one long-standing trustee brings up concerns about employees using procurement/credit cards for unauthorized purchases. David knows that there are numerous controls in place for the use of procurement cards and relatively few cases of misuse. Furthermore, the use of procurement cards has saved significant amounts of money by streamlining processes and eliminating paper document routing.

> Nevertheless, this trustee brings up the concern regularly. David asks the risk manager at the water cooler, “Is there some way to put the risks of procurement card fraud and misuse into relevant perspective compared to other much larger risks desperately needing time on the audit committee agenda?”

ERM is an ongoing effort requiring the commitment of all members of the institution. By implementing an ERM program, higher education institutions can improve their ability to identify, assess, and manage risks. This can help them to protect their assets, ensure the quality of their programs and services, maintain a positive reputation, and comply with regulations.

Here are some tips for implementing ERM in higher education:

- Get executive buy-in. ERM is most effective when it is supported by the institution's top leadership.
- Involve all stakeholders. ERM should be a collaborative effort that involves all levels of the institution.
- Use a risk management tool. There are a number of different risk management tools available that can help institutions to implement ERM.
- Communicate effectively. It is important to communicate the ERM process and its benefits to all members of the institution.
- Review and update the ERM process regularly. The ERM process should be reviewed and updated on a regular basis to ensure that it is still effective.

Focus Your ERM Efforts

- Don't try to cover every possible risk. It is impossible to predict and plan for every possible risk. However, by focusing on the risks that are most likely to impact your organization's strategic objectives, you can significantly reduce the chances of failure.
- Start with those that matter most for the success of your organization's strategic objectives. When prioritizing risks, it is important to consider the following factors:
    - The likelihood of the risk occurring
    - The severity of the consequences if the risk does occur
    - The importance of the objective that the risk could impact
- Develop action plans to mitigate risks. Once you have identified and prioritized your risks, you need to develop action plans to mitigate them. These plans should be specific, measurable, achievable, relevant, and time-bound.

- Understand which risk criteria are important to leadership. By understanding which risk criteria are important to leadership, you can have frank discussions about how much risk the organization is willing to take. These discussions can help to reveal where the organization may be culturally when it comes to risk-taking or risk aversion. This information can then be used to develop risk appetite statements, which can guide decision-making throughout the organization.

By following these tips, you can create a risk management effort that is tailored to the specific needs of your organization.

I. COSO, ISO, and the Role of Standards in the ERM Process

ERM has a reputation among some to be complex, labor intensive, and expensive. While it can indeed be all those things, there are also some key resources that can help make the process clearer, more efficient, and more sustainable. The most effective weapon against the ambiguity of ERM is standards. Standards are typically the result of years of work conducted by an interdisciplinary group of experts that articulate the key elements and characteristics that an ERM program should have. This section provides an overview of the role of standards, discusses the two primary ERM standards in use, and discusses how these standards can be used to design your institution's ERM program and articulate it in an ERM framework.

The Role of Standards

A standard is typically a document that provides information, requirements, rules, and guidelines for a particular process, product, or service. In the ERM world, there are two dominant standards in use: the ISO (International Organization of Standardization) 31000 2018 Risk Management Standard and the COSO (Committee of Sponsoring Organizations, of the Treadway Commission) Enterprise Risk Management - Integrating Strategy with Performance Framework (2017). For simplicity, in this section, we will refer to them simply as ISO 31000 and COSO.

There are several widely referenced ERM standard resources. The ISO has three risk management publications: (1) ISO 31000-2018 Risk Management provides a common approach to managing risk regardless of sector or industry which can be applied to any event or activity, including integrating risk into decision-making; (2) ISO 31010-2019 Risk Assessment Techniques provides guidance on the selection and application of techniques for risk assessment; (3) *Risk Management – A Practical Guide,* published in 2021 by ISO to assist organizations by providing guidance and direction on how to integrate an effective risk-based, decision-making framework into their governance, leadership, and culture.

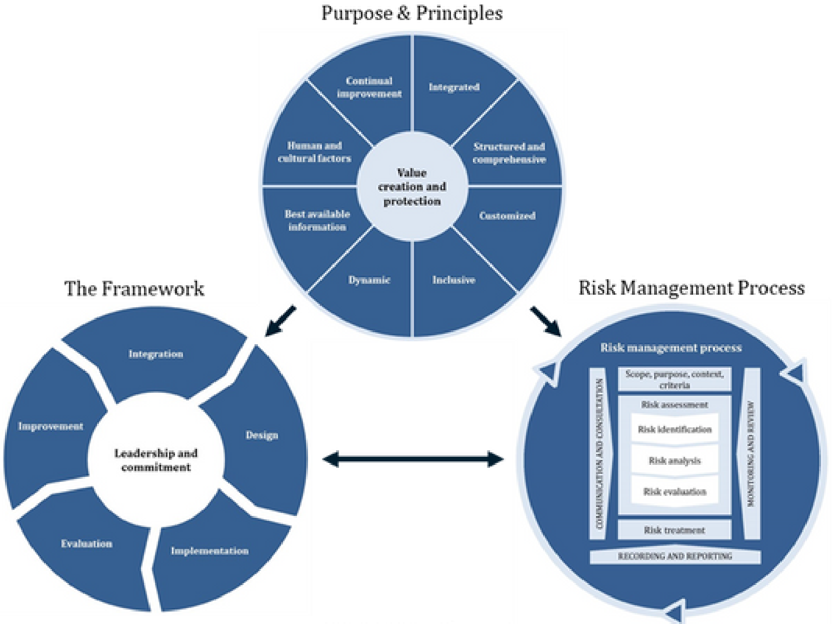
As a follow-up to its original 2004 document, COSO published in 2017 *Enterprise Risk Management– Integrating with Strategy and Performance*, which highlights the importance of considering risk in both the strategy-setting process and in driving performance, and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment.

ISO 31000

The ISO "is an independent non-governmental organization with a membership of 162 national standards bodies. Through its members, ISO brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international Standards that support innovation and provide solutions to global challenges."[1]

ISO 31000 was developed by ISO's technical committee on risk management, ISO TC 262. The inaugural version of ISO 31000 was published in 2009 and had representatives from approximately 25 countries. The 2018 revision had representatives from about 40 countries who had a risk management or operationally focused background or expertise and provided input. The committee consisted of representatives from universities, risk management-focused professional associations, state agencies, private and public corporations, insurance companies, and others.

ISO 31000 has three components, including the purpose and principles, the framework, and the risk management process, as illustrated here in Figure 1:



ISO 31000 – Figure 1

[1] ISO 31000 – Risk Management Overview Brochure, published February 2018, (https://www.iso.org/publication/PUB100426.html)

The “purpose and principles” establishes the primary objective of ERM as existing to create and protect value and articulates eight different characteristics of successful and effective ERM programs. Those characteristics include that the ERM program must be integrated, structured, and comprehensive; customized; inclusive; dynamic; act on the best available information; consider human and cultural factors; and be continuously improved.

The “framework” section is based on the “plan, do, check, act” cycle and is centered on leadership support and commitment. The framework represents the governance infrastructure that is built within the organization to drive risk management activities on an ongoing basis and serves to escalate and communicate risk across the organization as needed. It begins with designing a plan (or a framework) for ERM, implementing that plan, evaluating the success of that plan, identifying opportunities to improve the overall approach, and integrating those improvements on an ongoing basis.

The “risk management process” is the third component of ISO 31000 and outlines the approach an organization should use to identify, evaluate, and treat its risks. It begins with setting the scope, purpose, context, and criteria for the particular area being assessed. (This is basically setting guardrails around the assessment and selecting the correct “ruler” to measure risks.) This is followed by the risk assessment phase, where the organization identifies, analyzes, and evaluates the risk, ultimately determining what further treatment is required to adequately address the risk. This section also provides guidance on how to appropriately engage stakeholders in the process, how to test assumptions and integrate continuous improvement and effective decision-making principles into the process, and how to report and record the results of the risk assessment activities to organizational leadership and other stakeholders.

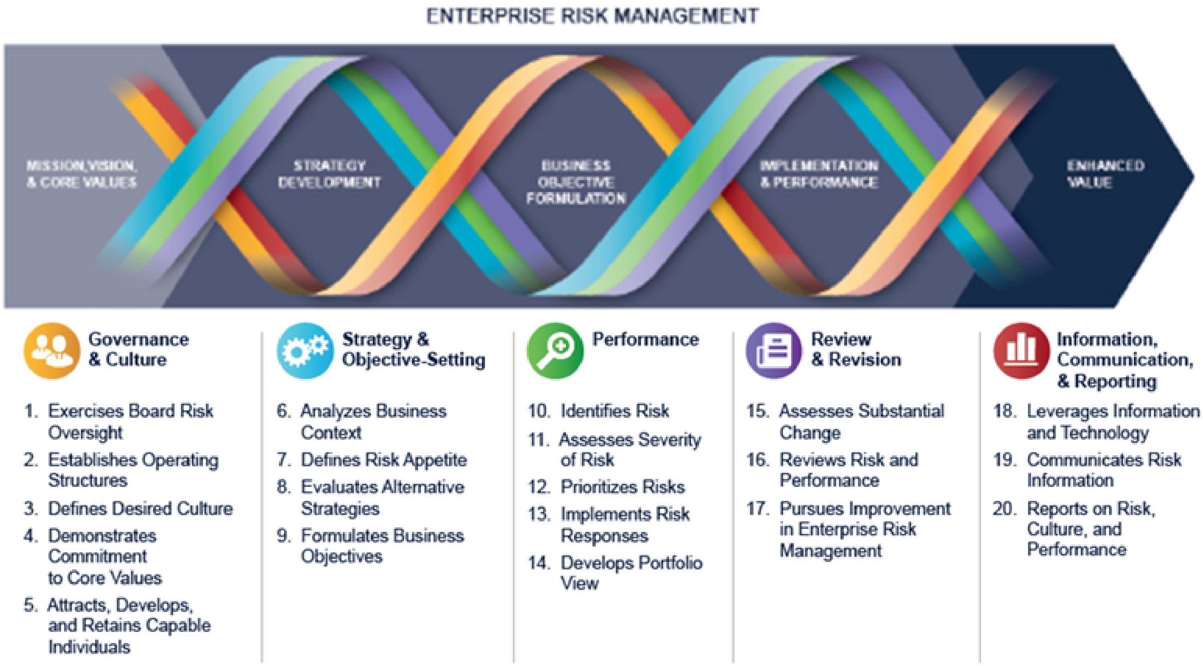
ISO 31000 provides a flexible, scalable approach to organizations of all kinds and draws an important correlation between the organization’s context (or environment) and how a shifting environment can impact an organization’s risk profile. Lastly, ISO 31000 emphasizes the importance of viewing risk as uncertainty- rather than a negative event- and acknowledges that risk can present both threats and opportunities that need to be managed effectively.

COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an organization “that is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations.”[2] COSO is a private sector initiative, jointly sponsored and funded by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, Institute of Management Accountants, and the Institute of Internal Auditors.

Though the organization leveraged a 21-person advisory council, the document was principally developed by PwC and has a strong corporate and North American-centric viewpoint. Given this lens/authorship, this framework leans more towards mitigation, structure, control, and compliance, rather than a risk management approach that can be more decentralized and organically integrated with decision-making. The COSO ERM framework was initially published in 2004, and later revised in 2017.

COSO highlights the importance of considering risk in both the strategy-setting process and in driving performance. It consists of five components and within these components are a series of 20 principles, as illustrated in the diagram below [3] :


ENTERPRISE RISK MANAGEMENT
MISSION, VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

[2] Enterprise Risk Management – Integrating Strategy and Performance, June 2017, https://www.coso.org/SitePages/Guidance-on-Enterprise-Risk-Management.aspx?web=1
[3] Enterprise Risk Management – Integrating Strategy and Performance, June 2017, https://www.coso.org/SitePages/Guidance-on-Enterprise-Risk-Management.aspx?web=1

The first part of this diagram shows two “ribbons” that connect an organization’s mission, vision, and core values with enhanced value and performance. The blue, green, and purple ribbons represent the organization’s strategy and objective-setting, performance, and review and revision activities and how they flow through common processes across the entity. The orange and red ribbons symbolize the organization’s governance and culture, and information, communication, and reporting activities, and represent supporting aspects of ERM. These processes/themes “wrap” around the organization’s strategic and business objective development process, and are used to implement and measure overall performance.

COSO connects risk and compliance functions in an organization and details how that collaboration can support the effective achievement of an organization’s strategy. It also makes a case for how an effective risk and compliance process can advise decision-making through deliberate articulation of risk appetite, and managing to an established threshold of performance. It views risks as “negative,” with opportunities primarily being focused on as part of strategy setting, and the overall framework is tailored to reduce and control threats to that strategy.

Summary

Both standards identify the critical ingredients for a successful and sustainable ERM program and offer specific guidance on the processes that should be put in place to support effective risk management. Both standards also emphasize the importance of tailoring the guidance to the specific culture, needs, context, and constraints of the particular entity. This act of tailoring the guidance from the standards and translating it to what ERM will “look like” for a given institution is done when the organization drafts its own ERM framework.

J. Explaining Maturity Models

One of the core features of an ERM program is the idea of self-assessment. An organization is challenged to identify risks and then make an honest assessment of whether they are sufficiently managing that risk. Risk maturity models take that self-assessment further and challenge ERM practitioners to assess the ERM program itself. Across the models, similar principles emerge as being key to understanding the maturity of a program.

- Where do your organization's leaders fall, on the spectrum of grudging attendance at another meeting about risk versus incorporating the principles of risk management into daily operations and decisions?
- Do members of your institution outside of your risk committee consider risk/reward trade-offs in routine decision-making?
- Have your processes been standardized? Are they repeatable and do they give your organization meaningful metrics and trend indicators?
- Is your program still testing the waters and learning?

These features do not always correspond to the "age" of the program. Having strong commitment and support from leadership and an appropriate governance structure are key factors even for programs that are just being initiated. Conversely, a program that has existed for years but is under-resourced, may find itself in the "initial" stages of maturity.

As previous sections have discussed, implementation of ERM in an IHE (or other organizational setting) is not one-size-fits-all. There are standards and frameworks that can serve as both starting points and aspirational endpoints depending on the culture, needs, and resources of your institution. Maturity models – and defining "maturity" – for an ERM program is no different. An important caveat is that none of the more popular maturity models are specific to the type of governance structures found in higher education institutions, and therefore a particular model may understate the institution's maturity due to the model's bend toward more corporate-specific governance and organizational structures.

Example Models

In 2006, the Risk and Insurance Management Society (RIMS) introduced its risk maturity model (updated in 2022), challenging programs to assess themselves across seven attributes determined to be core to a functioning ERM program. Under each attribute, the model provides competency drivers and indicators of the maturity of a program. Through the self-assessment, programs are able to rate their programs and arrive at one of five maturity levels: ad hoc, initial, repeatable, managed, or leadership. Like all aspects of ERM, the exercise of self-assessment is iterative. Programs looking to progress are able to use this exercise to set goals and track progress against them.

Other organizations have developed their own maturity models that take into account different features of the ERM process. For example, AICPA and CIMA co-developed an ERM assessment tool[4] that is grounded in the COSO framework and asks 75 questions under eight attributes of an ERM program. Their assessment is simple, asking only if the element is present or not, and then tallying up the number of elements a program has operationalized, which leads to one of four categories of "maturity" under their model.

More recently, the Organisation for Economic Co-operation and Development (OECD) in collaboration with the Internal Revenue Service (IRS) developed a model that focuses on ERM practitioners in the field of tax administration.[5] Like the AICPA and CIMA model, the OECD model includes eight attributes and returns a scored maturity in one of these categories: emerging, progressing, established, leading, or aspirational.

The attributes under evaluation in these models and a description of the different maturity levels (output of the assessment) are provided in tables at the end of this section to illustrate both the similarities and differences among the models. Some themes repeat across models, and some are unique framings. Other models have been developed and the examples here should not be read as an endorsement of one model over another.

[4] AICPA&CIMA CGMA Risk Assessment Tool, available at: https://www.aicpa-cima.com/resources/download/evaluate-enterprise-risk-management-maturity

[5] OECD (2021), Enterprise Risk Management Maturity Model, OECD Tax Administration Maturity Model Series, OECD, Paris. Accessed: https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/enterprise-risk-management-maturity-model.pdf

Considerations for Using a Maturity Model

Before using one of these or any other model, thought should be given as to what information your program or institution needs to get out of the exercise.

- Is this an internal-use exercise where the focus is to understand where you are?
- Is there a need for benchmark data and an understanding of how the maturity of your program fits among peer institutions?
- Is there support for continuing to build out the program? Is the goal of the assessment to identify specific areas or aspects of the process that could be improved?

Depending on the answer to these and other questions, you might select one model over another. For example, the RIMS model provides benchmark information from years of organizations using the model, but you may be able to get similar data from a firm your institution already does business with, or from peer groups. Similarly, the OECD model is careful to state at the beginning that “there is not a prescribed optimal level of maturity” that an organization must achieve, but that models should be used as a mechanism to understand their current state and can be used to structure conversations with other members of an organization as to what would be required to progress – if progress is a priority.

In February 2023, Deloitte produced a white paper discussing the four different model types[6] highlighting differences in approach, assessment, and outcome. Considering these factors before initiating an assessment of a program may be helpful in ensuring the output of the exercise is the information your program or institution requires in the context of goals for your institution’s ERM program.

An outline of the seven attributes and an overview of the concepts under each is provided in Figure 2 on the following page.[7]

[6] Accessed: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-public-sector-considerations-for-maturity-model-selection-v3.pdf

[7] Content in Figure 2 is adapted from RIMS State of ERM Report 2008, available at: https://www.sec.gov/comments/s7-13-09/s71309-121b.pdf, and the RIMS State of ERM Report 2015, available at: https://www.rims.org/resources/risk-knowledge/white-paper/state-of-erm-report-2015

Figure 2: Seven Attributes of a Functioning ERM Program

1 Adoption of ERM-based Approach

- Is there buy-in on using an ERM-based approach?
- Consider the extent of: executive support, risk ownership within business processes, and short vs. long-term approach to risk management (reacting to immediate risks vs. recognizing those on the horizon).

2 ERM Process Management

- How integrated is ERM into business operations and culture? Is there a consistent approach to and process for evaluating risk?
- Consider whether the ERM process is repeatable and scales with your organization's needs; the extent to which the process is defined; and how accountability is distributed in the organization.

3 Risk Appetite Management

- What is your organization's risk tolerance, and how is that informed? How is the balance of risk vs. reward evaluated?
- Consider to what extent there is awareness of trade-offs between risk and reward; to what extent is there appreciation for any gaps between perceived and actual risk and how that affects risk evaluation.

4 Root Cause Discipline

- Does your organization's process link outcomes (apparent risk) with a source (root cause)?
- Consider whether risks are evaluated on their face, or the extent to which root causes are identified, and the extent to which internal controls are implemented to mitigate those risks.

5 Uncovering Risks

- What is the scope of information evaluated in the organization's risk assessment of a threat or opportunity?
- Consider the extent of documentation evaluated when assessing risks and whether front-line risk owners are engaged in bringing information forward to develop risk mitigation strategies.

6 Performance Management

- How does risk mitigation inform the execution of an organization's mission and strategy?
- Consider whether goals are communicated such that business operations align with risk-informed goals for the organization, and whether performance indicators are developed from the ground up.

7 Business Resiliency & Sustainability

- Do ERM activities and plans feed into operational planning?
- Consider to what extent risk-based methodology informs and feeds into operations, business continuity, and resiliency planning.

Attributes Evaluated in Each Model

RIMS	AICPA & CIMA (CGMA)	OECD
Adoption of ERM-based approach	Risk culture	Strategy
ERM process management	Risk identification	Governance
Risk appetite management	Risk assessment	Culture
Root cause discipline	Articulation of risk appetite	Risk identification
Uncovering risk	Risk response	Risk analysis and evaluation
Performance management	Risk reporting	Risk treatment
Business resiliency and sustainability	Integration with strategic planning	Review and revisions
	Assessment of ERM effectiveness	Information, communication, and reporting

Maturity Levels Based on Model

RIMS	AICPA & CIMA (CGMA)	OECD
Ad hoc	Just Getting Started	Emerging
Initial	Basic ERM Practices in Place	Progressing
Repeatable		Established
Managed	Basic and Some Sophisticated ERM Practices in Place	Leading
Leadership	Robust ERM in Place	Aspirational

K. What if Your ERM Team Is…You?

Not every institution has a separate team or resources dedicated to ERM. In many instances, ERM may be only one of the responsibilities assigned to an individual. Although it may seem daunting, ERM is a journey – even small steps in the right direction can set you on the course of a successful program. Establishing an impactful ERM program takes sustained effort and commitment from individuals and groups across the organization. However, a program implemented with adaptability and resilience will bring meaningful, ongoing discussion and engagement that will serve the organization well. Here are a few suggestions to get you started on or continue to grow your ERM program.

Building a Case for ERM

Having a C-suite and board that believes in the value of ERM is the first step in establishing the foundation for a purposeful program. The events of the past couple of years have elevated ERM in the eyes of stakeholders, however, communicating why ERM is right for your organization is still an exercise worth undertaking. Build a case for how an effective ERM program can provide the institution with the processes and tools it needs to become more anticipatory and effective at evaluating, embracing, and managing the uncertainties it faces. Share case studies of peers who have implemented valuable ERM programs and point to the ever-growing community of higher education ERM practitioners. Getting your board and C-level stakeholders in alignment sends a powerful message to the rest of the organization that ERM is a key organizational priority.

Stakeholder Group
As a team of one, your primary role should be to facilitate risk discussions at all levels of the organization, using the framework (*refer to Section F for more information on frameworks)* as a consistent point of reference. A cross-functional group of stakeholders/risk champions who bring viewpoints from various areas of the organization can be instrumental in identifying and elevating enterprise risks. Leverage existing cross-functional working groups, councils, or committees to start with as it provides an easy way of integrating risk discussions into institution-wide initiatives. Individuals in these groups can also serve as a network of risk liaisons that can provide periodic updates on new developments in their respective areas or progress on risk management actions.

Tools
Join forces with one or several other teams within the institution to build a case for a governance risk and compliance (GRC) system (software-based ERM system). Several providers offer a suite of modules customized for different risk management entities within an organization, for example, audit, insurance, environmental health and safety (EHS), business continuity planning (BCP), and ERM. Adding an ERM module to an existing GRC system can be a cost-effective way to automate intake of risk identification, assessments, updates on risk, and corresponding mitigating actions by risk owners, and to provide effective, regular reporting capabilities. Keep in mind that it may take a while to find an ERM process that works for your organization. Make sure your process is not driven by the GRC tool, but rather that the tool can complement the process you have established.

Educate
ERM is a shared responsibility – as more people across the institution become familiar with the concept and framework of risk, day-to-day decisions tend to become risk-informed. Find opportunities to present the risk framework, process, and templates at orientations, team meetings, town halls, lunch and learns, etc. Use existing media for institution-wide communications (newsletters, collaboration sites, website tiles, etc.) to advertise ERM capabilities. Consider establishing "office hours" (a few pre-determined hours each week, online or in-person) during which people can reach out with ERM-related questions.

Evolve

Every ERM program is as unique as the organization that it is built for. Do not hesitate to obtain and implement feedback on tweaks and updates that make the program more user-friendly for the stakeholders in your organization. Once your program is in a place where stakeholders are familiar and comfortable with the process and framework, invite a group of peer practitioners to review your program and offer recommendations on evolving your program to a more mature version.

L. Using Technology in an ERM Program

In the field of ERM, technology has the potential to be a support or a distraction. When technology is aligned with your ERM program, it can be a driver of ERM program maturity; when not aligned, it can become an inhibitor of growth. There are many ERM-associated technologies on the market designed to implement a variety of functions and outcomes. As your institution contemplates technology to bolster your ERM program, first evaluate which ERM program goals and objectives you are seeking to support, enhance, or streamline through technology.

Ask yourself questions such as the following to narrow down what you are trying to achieve:

- Are we seeking to support, enhance, or streamline current ERM program processes? If so, which processes?
  - Are we seeking to increase the transparency of the ERM program, risk, and/or risk mitigation?
  - Are we seeking to better facilitate stakeholder engagement?
  - Are we seeking to create a central repository of ERM risk and/or mitigation data?
  - Are we seeking to actively monitor risk or risk management activities?
  - Are we seeking to assess the effectiveness of strategies?
- Are we looking for technology to push us to build new components of the ERM program?
  - How much change can the ERM program and stakeholders tolerate?
  - Are we ready for such change?
- What is our degree of readiness to implement the technology?
  - Do we have the right partners from our institution involved?
  - Are there any required integrations with any existing institution platforms?
  - Are we prepared to manage the new technology?
  - What training needs will accompany the implementation of the technology?

Having firm objectives will assist you in refining your search for technology and evaluating more objectively how well available options can support your program.

In addition to conducting your internal assessment, leverage your URMIA network to learn about your colleagues' experiences, lessons learned, and best practices related to the implementation of technology for their ERM programs. Colleagues are often willing to share their perspectives and to allow you to build off their work in furtherance of the field of ERM. When one program is doing well, it lends the potential for other programs to follow suit.

Even with – or maybe even because of – this degree of preparation, you may not find a technology on the market that suits your needs. The bells and whistles that come with some platforms may not align with your objectives and may, in fact, distract from your objectives. Sometimes the "nice-to-haves" that come with certain technologies can take away the focus on the "need-to-haves" required to move your program forward. Even more problematic may be components of technology that are more aspirational than your program can integrate, potentially taking you down a path of maturity that either isn't a priority for your program or for which your program is not ready.

If you do not find a technology solution on the market that meets the vast majority of your ERM program's needs and objectives, do not move forward with that technology. Instead, consider what in-house capabilities you may have that can create tools that can be designed to better align with your program. Technology need not always be complex or highly sophisticated to help you meet your objectives. It merely needs to align with your ERM program goals and objectives.

In summary, make the investment to prepare for a search for ERM technology. Gathering and reflecting upon your requirements will serve your institution and your ERM program well. Ultimately, affirming where technology can align with your program needs can prevent pitfalls and assist in identifying support that can interconnect with, rather than divert from, your ERM program.

M. The Overall Role of Risk Management Within the Organization

The role of the risk management professional within the higher education environment varies from institution to institution. However, there are common threads in terms of what the role should accomplish including mitigating risk to protect the life safety, reputation, finances, operations, and assets of an entity through techniques of risk identification, transfer, risk treatment, and risk control. If done well, a trained risk professional will help take the board and executive vision and provide guidance to enhance a risk-aware culture throughout the organization, where everyone is ultimately a risk manager.

This requires a level of awareness and general understanding on many levels including the strategic goals of an organization, the drivers to achieve those goals, and the ability to inspire line managers and staff to embed risk mitigation techniques into their processes. It also requires a level of creativity to thread disparate concepts into an assessment of risk - or opportunity - and, much like bench chemistry, assess whether or not they will mix well or provide a compromising position. In doing so, the risk professional must embrace the expertise of those who conduct the work each day and support them in implementing better outcomes for their responsibility areas where issues have occurred. This will create confidence in those who manage and a risk-aware culture that spreads throughout the entire organization.

Being a risk professional is something that is not done in a vacuum or behind a desk, rather is one of coaching, encouraging, and building confidence in an organization on a day-to-day basis. Skill sets include being a project manager for the implementation of programs or the annual renewal of insurance programs. Yet when an incident occurs, it can be a position that, through prior training, planning, and building confidence, can help an entity get through a bad situation without harming its reputation or bottom line. Incidents will happen but how well-prepared an entity is will determine its outcome and success.

N. The Role of the "Risk Owner"

Many educational institutions have employed a person or office with responsibility for oversight of managing the organization's risks. Resource-rich institutions may have a person dedicated to this or even a team while others may have one person managing risks along with a cadre of other responsibilities, perhaps without 'risk management' even being in their title. At the end of the day, it doesn't matter who has the operational responsibility for managing risks, because - with an ERM program or not – everyone is a risk manager!

A "risk owner" is every administrator, dean, department chair, unit leader, director, manager, supervisor, or other leader who has the responsibility to deal with risks and issues that are specific to their function or area. It is they who – consciously or subconsciously – evaluate the risks at the operational level and make decisions on how to manage those risks.

In the case of ERM, risk owners play vital roles in identifying, evaluating, and mitigating risks in their area, and are ultimately accountable for facilitating their ERM risk assessment. This is certainly done in concert and partnership with the others involved in overseeing the ERM framework, such as the risk manager, though it is important to recognize that the centralized oversight of ERM necessitates local ownership by the risk owners. ERM simply is not a one-person job, nor it is a point-in-time exercise. It is ongoing and the best outcomes happen when ERM is operationalized at all levels of the institution. In addition to conducting the ERM risk assessment itself, the goal for most risk owners is to embed mitigation techniques in ongoing programs, make improvements in processes and programs, and inform prioritization and decision-making.

The following details the core functions and responsibilities of risk owners with the above in mind:

- Risk Identification – Risk owners identify the risk in their areas, mindful of those that may be inherent to the higher education industry versus those that are specific to their institution. Though assessing for their area, risk owners also consider risks integrated or correlated with other areas across the institution. It is ERM, after all. In fact, some institutions identify risks as part of combined efforts through a series of interviews with key stakeholders. Risk owners should validate these efforts to determine if the risk identified best captures the environment for their area. This - as with many other aspects of ERM - is a continual exercise as the world around us evolves, new trends emerge, and the risk landscape is in perpetual change.
- Risk Evaluation – Once risks are identified, the risk owner evaluates each risk using the preferred ERM framework for the institution. This may include defining the risk, scoring the risk for probability and impact, and categorizing the risk (e.g., operational, reputational, strategic, financial, regulatory, etc.). Risk response strategies can be determined from the risk owners' evaluation. For example, risk owners can determine (often by the mapping of risks scored) whether a risk should be mitigated (high-risk score), monitored/optimized (moderate risk score), or tested/assured (low-risk score) dependent upon the scoring.
- Risk Mitigation – The risk identification and evaluation processes take into consideration the mitigation activities in place for the institution. Examples of potential mitigation activities that a risk owner may highlight include policies and procedures, training, controls, or monitoring. Risk owners not only document current and future mitigation activities but also assess how the mitigations impact scoring and determine the residual risk to the institution. Additionally, risk owners ensure that the mitigation activities are being conducted and proposed mitigations are implemented according to identified milestones to reduce the likelihood or impact of a component risk.

The formal ERM framework may require risk owners to present the assessment to various committees or leaders, including at the board level, or report/track efforts through a formalized process. This creates an opportunity for the risk owners to highlight the ERM efforts and provide an organizational overview of their area.

As with risk managers, risk owners do not have to take on the steps above alone. ERM outcomes are improved with the involvement of all stakeholders and the risk owners can help influence by engaging others in their area and across the institution in the steps above. Also, risk owners can utilize the ERM framework as part of the operations and strategies for their unit, identifying key performance indicators, and using them for prioritization and decision-making as noted.

Risk-Informed Decision Making

Decisions should be informed by an appropriate assessment of risk. Sustainable organizational success can only be achieved through informed and structured decision-making, including when setting the organization's objectives and planning, implementing, executing, evaluating, and improving the organization's strategy.

Decision-making needs to consider risk from both external and internal sources, as organizations and their objectives are affected by many factors, often outside their direct control. Risk management should, therefore, be an integral part of these decision-making processes at every level of an organization and across all operations (i.e., “built-in”).

Here are some specific ways to improve the decision-making process in an organization:

- Identify the risks that could impact the organization's ability to achieve its objectives. What could go wrong?
- Assess the likelihood and impact of each risk. How likely is it that the risk will occur? How much damage would it do if it did occur?
- Develop risk mitigation strategies. What can the organization do to reduce the likelihood or impact of each risk?
- Incorporate risk management into the decision-making process. When making decisions, consider the potential risks and how they could impact the organization's objectives.
- Monitor and review the risk management process on an ongoing basis. Are the risk mitigation strategies working? Are there any new risks that need to be considered?

By following these steps, organizations can improve their ability to make informed and structured decisions that are less likely to lead to negative consequences.

O. Integrating ERM into the Business Model for the Long Term

While thorough planning and solid support for ERM implementation is a must, sadly many ERM programs have fizzled out after a year or two. Practitioners must plan beyond the early phases of building an ERM program to ensure progress is sustained and ERM is integrated into the institution's culture. Momentum can fade and ERM supporters instrumental in the program launch may retire or rotate out of their positions of influence, causing the ERM idea and corporate understanding and vision of what it is to accomplish to dissipate. Higher education institutions are constantly experiencing new initiatives, marketing campaigns, and shifting priorities dictated by stakeholders or by senior leaders. Caution must be taken to avoid having the ERM program slowly migrate into the graveyard of past experiments or faddish trends that didn't get fully integrated into the institutional culture and lacked staying power.

There are some successful strategies that will help an ERM program become resilient and sustainable. Linking the ERM framework and processes to institutional governance, as one of several management activities that provide assurance of adequate management control and corporate risk awareness, highlights its significance. Additionally, both internal and external stakeholders desire good stewardship of resources. ERM helps with the management of budget and personnel resources by prioritizing larger enterprise-wide risks and building the risk intelligence of decision-makers, so that responses to both opportunities and threats are more rational. This helps avoid either over- or under-resourcing risk treatments and controls.

Connecting ERM's purpose and outputs to other enduring processes like strategic planning, the budget cycle, accreditation review, annual audit plan development, external financial statement audits, bond ratings, and program reviews help to keep risk considerations and risk effects in the discourse across departmental and functional lines.

Carefully synchronizing the release of ERM reports and process outputs when they will be most valuable for these other administrative and academic cycles will create a demand and expectation for ERM to "be there."

Some proven actions and techniques to help ensure an ERM program remains vibrant and enduring include:

- Don't try to implement ERM across the entire organization all at once. Start with a small pilot in one department or division. This will help you to identify the challenges and opportunities associated with ERM implementation.
- ERM is most effective when it is supported by senior management. Get senior leaders involved in the ERM process who are committed to the initiative and who are willing to allocate the necessary resources. This will help to ensure that ERM is a priority for the organization.
- Have a succession plan in place for the person currently acting as the ERM lead so the next person or persons can take the handoff without interruption to avoid a program stall.
- Establish an accessible archive of ERM legacy materials and implementation history on a shared drive or collaborative site.
- Establish a risk committee with a defined charter. Seek its formal recognition and written term appointment letters for members issued ideally from the president's/chancellor's office.
- Create and gain approval at the cabinet level of a risk philosophy for the institution – bonus if you can get a risk appetite statement agreed upon and approved as well.
- Develop an ERM handbook for risk committee members and an ERM policy or regulation.
- Develop an accepted ERM terminology lexicon with definitions of key terms and phrases to help unify thought and reduce confusion related to ERM activities and conversations.
- There are a number of GRC technology solutions that can help organizations to manage risk more effectively if you have the financial and support resources to consider implementing them. These solutions can help automate tasks, improve communication, and provide insights into risk trends. Use a risk management tool that is appropriate for the size, complexity, and needs of the organization.
- Ensure the risk committee conducts its business with formality to include action-tracking, minutes, and adequate representation from all major business units and departments of the institution. This will come in handy as memories fade.

- Regularly report directly or through channels to both the cabinet and at least the appropriate governance (board) committee with risk/compliance oversight responsibility, if not to the full board.
- Have ERM or risk specifically mentioned in the appropriate governance body (board) committee title and charter language, to ensure the risk management aspect of oversight is distinct from audit, finance, or compliance.
- Include ERM specifically in the job description and perhaps even in the job title of the risk manager or person designated as ERM lead.
- Adjust proposal and initiative presentation steps to senior leadership to include required risk committee or ERM review and input prior to their being considered.
- Publish periodic communications both to the campus community (on general ERM topics and best practice risk treatment ideas) and occasional executive-level communication (on ERM areas of interest for senior leaders and governance officials) to raise awareness and demonstrate the value of relevant risk information gained through the ERM program.
- Engage regularly with administrative and academic groups to provide tailored risk assessments, and risk trends and to receive feedback on risk issues (deans and directors, athletics, extension programs, etc.).
- The ERM process is not a one-time event. It is important to continuously monitor and improve the process to ensure that it is effective in managing risk. This may involve making changes to the risk management framework, the risk management tools, or the way that risk is managed within the organization.
- Include ERM considerations in department/unit strategic plans.
- Consider how risk management wording might be included in evaluations and performance reviews.
- Propose a “Tone at the Top” message to the campus from the president or chancellor highlighting the progressive value of an ERM approach with a description of a culture where “everyone is a risk manager.”
- The risk landscape is constantly changing so it is important to review risks regularly and make changes as needed.
- ERM is an ongoing process that takes time to implement and mature. Be patient and persistent with ERM implementation. With time and effort, ERM can be a valuable tool for organizations that are looking to improve their risk management capabilities.

P. Successes and Pitfalls

There may not be one tried-and-true ERM approach that you can immediately adopt however, these are a few common practices that can assist with the successful implementation of an ERM program at your institution.

- Start with strategic objectives (or organizational mission) - Using the strategic objectives of the organization as a north star ensures that everyone is striving for the same goal and recognizes risks that can impact the achievement of those objectives. However, not every issue or concern identified during risk discussions is a threat to the achievement of strategic objectives. Clearly laying out criteria that define enterprise risks and their prioritization is key to the efficiency of an ERM program.
- Pilot an assessment - Completing a risk assessment for a department, academic unit, or lab can be an effective way of creating a blueprint for risk assessments while demonstrating the value that ERM can bring to the organization. This also helps identify and iron out any wrinkles in the process and sets you up with a case study that can be shared with the rest of the organization.
- Partner with other risk management functions - Clarify and communicate the roles and responsibilities of the different offices that play a role in facilitating risk management activities across the organization, such as audit, insurance, compliance, general counsel, etc. Having an open channel of communication and information-sharing between these offices helps with quick identification of emerging issues, and elevation of serious risks in a timely manner.
- Identify the future state - Apart from identification, prioritization, and reporting of key risks, it is also important for risk owners to determine a desired future state for their respective risk areas. This ensures accountability for risk management actions and helps set up a cadence through which progress on risk mitigation activities can be tracked and reported, thus demonstrating ERM at work.

- Build awareness - As mentioned before, ERM is a team sport – greater involvement and engagement equals more informed risk-taking and decision-making. Get your message out on the road, grab every opportunity to raise awareness, and educate the community on the risk management framework and resources.

And here are a few areas to watch out for to avoid tripping up your ERM program:

- Lack of executive support - A successful ERM program is very much driven by “tone at the top.” Not having the support and buy-in of senior officials is a surefire way of bringing your program to a grinding halt. Being able to demonstrate the value that ERM provides - not just while setting it up, but throughout the ERM journey - is the best way to keep senior officials engaged and onboard.
- Don’t try to fit a square peg into a round hole - What works for one organization may not work for another. Every ERM program is unique and should be built around the needs and culture of the organization. Although learning from peers and leveraging successful practices can be effective, be ready to tweak those practices so that they are aligned with your organization’s culture and goals. Another pitfall is a lack of alignment between risk management and the organization's objectives. If risk management is not aligned with the organization's objectives, it will be difficult to make effective decisions about how to manage risk.
- Avoid jargon - ERM jargon can be overwhelming and off-putting to those who are new to the process. When trying to get buy-in, try using commonly used terms that people in the organization are familiar with. For example, ERM itself may not be a preferred moniker, and in some institutions, the process is referred to as integrated risk management, the office of risk management, the system of risk management, or others. Similarly, impact, likelihood, and velocity may be replaced by a different framework to prioritize risks based on the organization's focus areas.
- Administrative burden - There is nothing that will discourage people more than adding to their workload. Try to use existing avenues such as team or committee meetings, technology, reports, and organization structure to integrate ERM into the fabric of the organization.
- Over-focus on risk avoidance - One of the biggest dangers of risk management is that it can lead to an over-focus on risk avoidance. This can stifle innovation and creativity and prevent organizations from taking calculated risks that could lead to significant rewards.

- Don’t let perfect get in the way of good - When you start out, you may have a vision of what you want your program to look like and how you want that program to function. However, as with any process, change is a constant and you will need to adapt to and prepare for several iterations before you get to somewhat of a steady state. Start small, get a few quick wins, and adjust and learn along the way. Having a program that people are aware of and can reference as they participate in the process is more valuable than waiting to get to an elusive ideal.

Q. Appendices - Additional Resources

- URMIA – of course! The URMIA Library has a wealth of resources– at the time of this resource's publication, the ERM folder itself within the URMIA Library listed 31 individual documents and presentations. You can find the library on the URMIA.org main page under "Resources." Other significant sources (also under that same Resources tab) include the "Enterprise Risk Management" tab within the URMIA Resource Guide and the URMIA Risk Inventory. Additionally, in the "Past Conferences" folder within the URMIA Library, there are numerous presentations on ERM that may be helpful to members just starting an ERM program.

- *ERM in Higher Education*, URMIA white paper, 2007.

- *Top Strategic Issues for Boards, 2022-2023*, AGB 2022.

- *Risk Management: An Accountability Guide for University and College Boards*, Janice Abraham, published by Association of Governing Boards, Second Edition, 2020.

- International Organization for Standardization, ISO, www.iso.org.

- Committee of Sponsoring Organizations of the Treadway Commission, COSO, www.coso.org.

- Association for Federal Enterprise Risk Management, AFERM, www.aferm.org.

- *Developing a Strategy to Manage Enterprisewide Risk in Higher Education*, National Association of College and University Business Officers (NACUBO), 2000.

- ERM Maturity Models
  - RIMS
  - Aon
  - AICPA & CIMA CGMA Risk Assessment Tool
  - OECD Enterprise Risk Management Maturity Model

- North Carolina State University Business School ERM Initiative
  - "REPORT: Executive Perspectives on Top Risks for 2023 & 2032"
  - “Revamping ERM: How Seven Companies Improved ERM Effectiveness” NC State Poole College of Management ERM Initiative (auth: Baker, Kreibich, Melendez, Robinson), 2022
  - Enhancing the Future Relevance of ERM: Insights from ERM Leaders

- Materials from Deloitte, Protivity, Beazley, and other organizations

- “Effective measurement of enterprise risk management programs,” Alberto G. Alexander, Ph.D., MBCI, ContinuityCentral.com, 2022

- Significant ERM advancement work has also been accomplished by AFERM, and Federal Government mandates for ERM programs within Federal agencies (Office of Management and Budget Circular A-123).

ERM RESROUCE

We thank you for your continued support in our efforts to contribute to ERM and risk management professional development materials in higher education.

CONTACT

URMIA
PO Box 1027
Bloomington, IN
47402-1027
Phone: (812) 727-7130

www.urmia.org
urmia@urmia.org
@URMIANetwork

URMIA
UNIVERSITY RISK MANAGEMENT & INSURANCE ASSOCIATION
HIGHER EDUCATION RISK MANAGEMENT