Enterprise Risk Management Handbook

June, 2010

Table of Contents

Overview 4
What is Enterprise Risk Management? 5
Why Undertake Enterprise Risk Management? 6
Draft UW System ERM Vision, Mission, and Objectives 7
ERM Value Proposition 10
Draft University of Wisconsin System Risk Council Charter 11
ERM Risk Reporting Process (Year 1) 12
Annual ERM Cycle 13
Identifying Risks 14
Assessing Risks 15
Impact and Materiality 16
Likelihood 17
Sample Risk Map 18
Risk Control Effectiveness 19
Risk Retention, Risk Mitigation, and Risk Ownership 20
ERM Risk Mitigation Process 21
Glossary 22

This Handbook is the property of the UW System, is private and confidential, and may not be copied, referenced or otherwise distributed to any person without the express written authorization of the UW System Legal Department.

Working Together to Proactively Manage Risks that could Threaten our Mission

As a state-wide university system, the University of Wisconsin's risk profile is complex and managing those risks is more important than ever. In the continuing effort to improve enterprise-wide controls and governance, we have begun the implementation of an Enterprise Risk Management (ERM) within the University of Wisconsin System through a pilot initiative.

The origins of the ERM initiative can be found in the need to align declining resources with mission-critical tasks, respond to the evolution of traditional risk management to a more cross-functional approach, and address increasing accountability standards driven in part by the Sarbanes-Oxley Act. The UW System Administration Offices of Operations Review and Audit and Safety and Loss Prevention have been the primary project lead to date, but success of this initiative will be determined by the level of participation received from all levels of the UW institutions and System Administration.

Enterprise Risk Management is a tool that will provide us with a common language and set of standards to identify, evaluate, prioritize, and manage ongoing risks that are inherent in our operations. Our goal is to develop an ERM structure that will expand the understanding of risk from traditional hazards, which can be transferred with insurance coverage, to include strategic, operational, and financial risks, while integrating risk ownership at all levels of the organization.

UW System has contracted with Arthur J. Gallagher Risk Management Services, Inc. and Core Risks Ltd. to help in the development of a project structure that will facilitate the identification of critical risks, provide a means to establish risk management priorities, and develop strategies to manage identified risks.

Overview

Generally speaking, Enterprise Risk Management (ERM) is an overarching process that will provide a methodology, a common language, and a set of standards to identify, evaluate, prioritize, and manage risks inherent in our operations. However, it is critical to note that just as every UW institution is different, so must their respective Enterprise Risk Management Program be unique – specially tailored to take into account the culture, structure, mission, and objectives of the UW institution and its stakeholders.

In the following pages, you will learn more about ERM and the tasks that we, as a university system, will undertake as we integrate ERM principles and practices into our operations. UW staff play an important role in helping to define what ERM will represent for the System and its campuses and in leading our efforts to develop an effective, sustainable ERM program that will become integrated into operations, as well as our annual review and budgeting process.

The ultimate success of our ERM Program will remain dependent upon your continued support, guidance, and input. As an overview, below is a summary of the ERM process:

Phase 1 – Program initiation – Establishment of Institution Core Working Group –
Definitions, Process, and Materiality
Pilot implementation:

- Conduct institution orientation session
- Interview Senior leaders and questionnaires to campus faculty, staff, and students.
- Compile interviews and questionnaires to develop a "Perceived Risk Map".
- Compile ERM Risks and conduct risk validation workshops – Assess output of interviews and questionnaires – identify and discuss other risks. In the workshops, we're going to review and validate previously-identified risks, identify additional risks, determine which have the highest priority, decide which require active management, and assign responsibility for developing plans and budgets to mitigate those key threats.
- Compile workshop results – provide feedback to campus Core Working Group and UW System Administration.
- Determine future UW System roll-out and plans based on pilot institution experiences.

Phase 2 – Ongoing UW System ERM Pilot Initiative and Institution Integration

By the end of the initial cycle, these mitigation plans and budgets will be consolidated in an Annual Risk Report for participating institutions. Mitigation plans, including needed resources, will be identified and incorporated into the institution's budgetary process. The ERM process will then move into an annual, ongoing cycle.

What is Enterprise Risk Management?

Enterprise Risk Management (ERM) is our comprehensive program to identify and manage – proactively and continuously – real and potential threats and opportunities that may affect our operations, both locally and globally.

Threats include not only ***dangers*** that could imperil our operations, but also the failure to take advantage of ***opportunities*** that could help us fulfill our mission and prosper. Both kinds of risks are important. Often, the risks identified through the ERM process will have already been previously identified. However, ERM allows for risks to be validated by a cross-functional representation of the institution and to properly place the risk within the context of other identified risks.

ERM augments current controls and capabilities to protect and increase stakeholder value and strengthen our work culture. The goal is to promote continuous, sustainable improvement across the System, creating value and competitive advantages.

The University of Wisconsin System's ERM program will be both strategic and operational:

Strategic: The ERM program will provide a consistent method to evaluate risks and opportunities and make more efficient use of assets, while meeting governance expectations.

Operational: The ERM program will provide each area of our operations with a methodology to identify, understand, and manage risks and opportunities in a manner that's consistent with UW's overall goals, objectives, and culture.

The result → Our ERM program will provide a fact-based, prioritized approach to risk management, allowing all of us to confront and examine our assumptions about risk and the steps we take to manage and mitigate risk. ERM is a disciplined process that draws on a broad base of cross-functional skills and expertise.

Why Undertake ERM?

Among the many reasons for pursuing an ERM structure are:

- The reality of reduced resources and increased accountability requiring better alignment of limited resources
- Responding to increased competition
- Improving strategic planning efforts
- Responding to the increasing number and diversity of risks related to higher education
- The need to meet good governance and accountability standards

ERM will also allow UW System to transition from traditional view and response to risk to one that is cross-functional and integrated throughout the organization.

Traditional Risk Management	**to**	**Enterprise Risk Management**
Fragmented		Integrated
Negative		Positive
Reactive		Proactive
Ad hoc		Continuous
Historical-looking		Forward-looking
Cost-based		Value-based
Narrowly-focused		Broadly-focused
Risk Silos		Systematic
Functionally-driven		Process-driven

Draft – UW System ERM Vision, Mission, and Objectives

Vision Statement:
The University of Wisconsin System endeavors to lead higher education by integrating the principles of Enterprise Risk Management (ERM) into the culture and strategic decision making of its academic, student affairs, and business functions. ERM will promote the success and enhance the accountability of the UW System by incorporating risk assessment into the System's strategic objectives and budget development process.

Mission Statement:

The mission of the University of Wisconsin ERM Pilot Project is to initiate a comprehensive program which will support the identification of the UW's mission-critical risks, assess how to manage those risks, and align resources with risk management responsibilities. The UW Enterprise Risk Management Core Working Group, in collaboration with other UW staff and a consulting firm, will pilot an ERM project at UW-Whitewater while continuing to support ongoing efforts at UW-Oshkosh and UW-Superior.

Goals and Objectives for Accomplishing the Mission:
Goal #1: **Integrate ERM into the culture and strategic decision making processes of the organization.**

Objectives:

1-1. Develop common ERM terminology.
Measures of progress toward meeting the objective:
- Has an ERM glossary been created?
- To what extent have the words associated with risk been defined and communicated among key staff, such as the Core Working Group, institution participants, System president, and cabinet.

1-2. Raise awareness of the need for risk management.
Measures of progress toward meeting the objective:
- Has the importance of accepting risk management responsibility been discussed among key staff?
- Long-term: Have employee orientations related to risk management been scheduled? Is an online self-assessment tool available for employees?

1-3. Establish continuous monitoring and communications processes.
- Measures of progress toward meeting the objective:
- Is an ongoing risk monitoring process in place?
- Is monitoring assigned to specific individuals who also communicate the results of the monitoring activity to appropriate levels in the organization, such as the chancellor, or president?

- Have formal communication mechanisms, such as a central web site or newsletter, been established? Is communication occurring on a regular basis?

Goal #2: **Balance the cost of managing risk with the anticipated benefits.**

Objectives:

2-1. Define the organization's overall risk appetite/tolerance, and establish associated materiality thresholds.
Measure of progress toward meeting the objective:

- Have management discussions occurred, with decisions made about how much risk the organization is willing to accept in key areas?

2-2. Document current procedures, controls, and risks.
Measure of progress toward meeting the objective:

- Has systematic documentation of risks and controls occurred in all functional areas of the organization, such as academic, financial and human resources, or in major risk categories, such as reputational, operational or strategic?

2-3. Compare current risks to control efforts, as well as to the organization's risk appetite, to help identify priority risks.
Measure of progress toward meeting the objective:

- Has the risk analysis resulted in the identification of the organization's top risks?

2-4. Assess the value of alternative risk management actions.
Measures of progress toward meeting the objective:

- Have alternative risk management strategies been identified for all of the identified the top risk areas?
- Do strategies respond to changing social, environmental, and legislative conditions?

Goal #3: **Manage risk in accordance with best practices, and demonstrate due diligence in decision making.**

Objectives:

3-1. Assign responsibilities for risk management at the "lowest" levels of the organization.
Measures of progress toward meeting the objective:

- Has responsibility for managing risks been assigned?
- Are Risk owners specifically assigned and accountable for remediation of identified and prioritized risks?
- Have action/response plans for each selected risk been created and assigned?
- Are actions taken tracked and reported?

3-2. Regard compliance with the law as a minimum standard.
Measure of progress toward meeting the objective:

- Has compliance as a minimum standard, to be exceeded if possible, been communicated to those in the

organization who track compliance?

3-3. Streamline risk-management-related practices.
Measure of progress toward meeting the objective:

- Have any risk-management-related or other internal control measures/activities been identified for elimination?

3-4. Identify competitive opportunities.
Measures of progress toward meeting the objective:

- Have benefits of assuming additional risk been identified?
- Have competitive needs or reputation been discussed at a strategic level?

Goal #4: **Use the pilot projects to develop a systemwide ERM implementation strategy.**

Objectives:

4-1. Establish an organizational and communication structure for managing the pilots.
Measure of progress toward meeting the objective:

- Is a structure in place to enhance planning efforts among the consultant, UW System Administration, and the institution contact people?

4-2. Transfer knowledge from the consultants to UW System Administration staff.
Measure of progress toward meeting the objective:

- Are UWSA staff well prepared to apply what was learned from pilot experiences to the next ERM phase?

4-3. Involve the UW System president and cabinet in ERM-related decisions.
Measure of progress toward meeting the objective:

- Is a communication strategy in place for informing the president and cabinet of ERM progress and for seeking feedback, when appropriate?

ERM Value Proposition

The value proposition – An Effective Management Tool:

1. ERM not only protects value but helps to create value for all stakeholders;
2. Establishes a defined framework and process for objective risk assessment and prioritized risk mitigation, *including identification of potential opportunities;*
3. Enhances our ability to achieve our strategic objectives; “risk-enhanced” budgetary process;
4. Creates a common risk language that enables comparative assessments of varying kinds of Strategic and Operational risk (e.g. Academic, Administrative, Student life, Financial, etc.);
5. Allows senior leadership to optimize the allocation of limited resources using pre-determined quantitative and qualitative methodologies.

University of Wisconsin System Risk Council Charter

Council Purpose -.

Operating Activities -

Duties of the Risk Council shall include:

Sponsor(s)/ Champion(s):

Chairperson:

Membership:

Stakeholders:

Meeting Frequency:

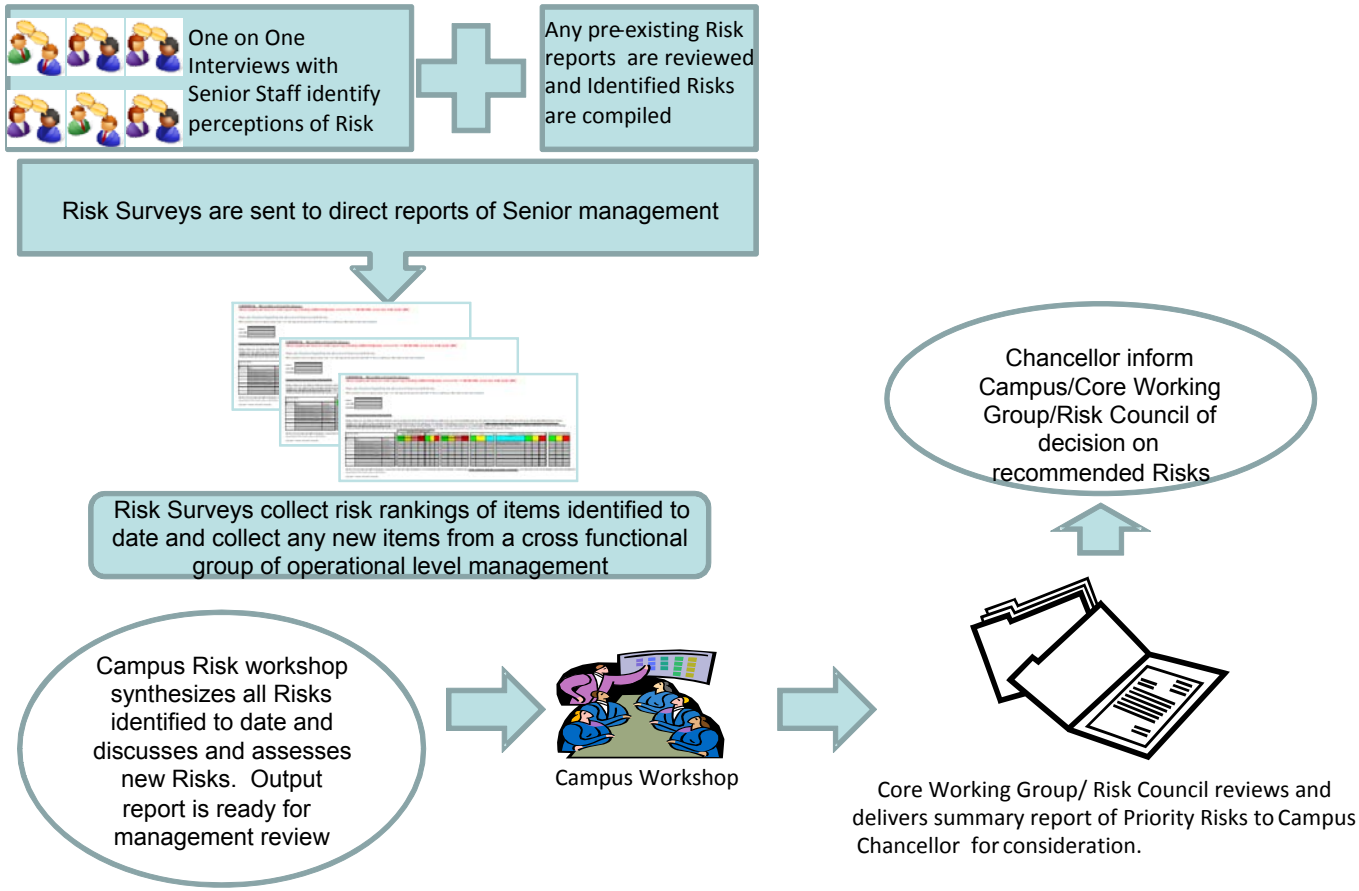
Authority:

Interpretation:

Note to reviewers of this handbook draft: It is anticipated that as the pilot phase progresses, the UW System Core Working Group will develop into a Risk Council. This page is intended to serve as a placeholder to help frame future discussions involving the formation of a Risk Council.

ERM Risk Reporting Process (year 1)

This chart represents the reporting/communication lines for the initial Pilot ERM reporting process.



Proposed Annual ERM Cycle

The first step in ERM is to identify threats which could materially impact our operations.

Some risks are common to all businesses, such as the risk of natural disaster, the risk of theft or fraud, or the risk of losing a competitive advantage. Other risks are peculiar to Higher Education, such as the risks associated with reputation/academic standing, and residential living for young adults.

Here are some common types of potential threats that UW faces every day:

- Closure of campus/building
- Damaging reports in the news media
- Credit crisis reducing availability of student loans
- Student health and safety

A risk can be managed in two ways:

Risk Retention

If an identified Risk is within Risk Retention, then current controls are retained, maintained, and monitored.

Risk Mitigation

If an identified Risk is not within Risk Retention, then further Mitigation controls are planned, prioritized, and implemented.

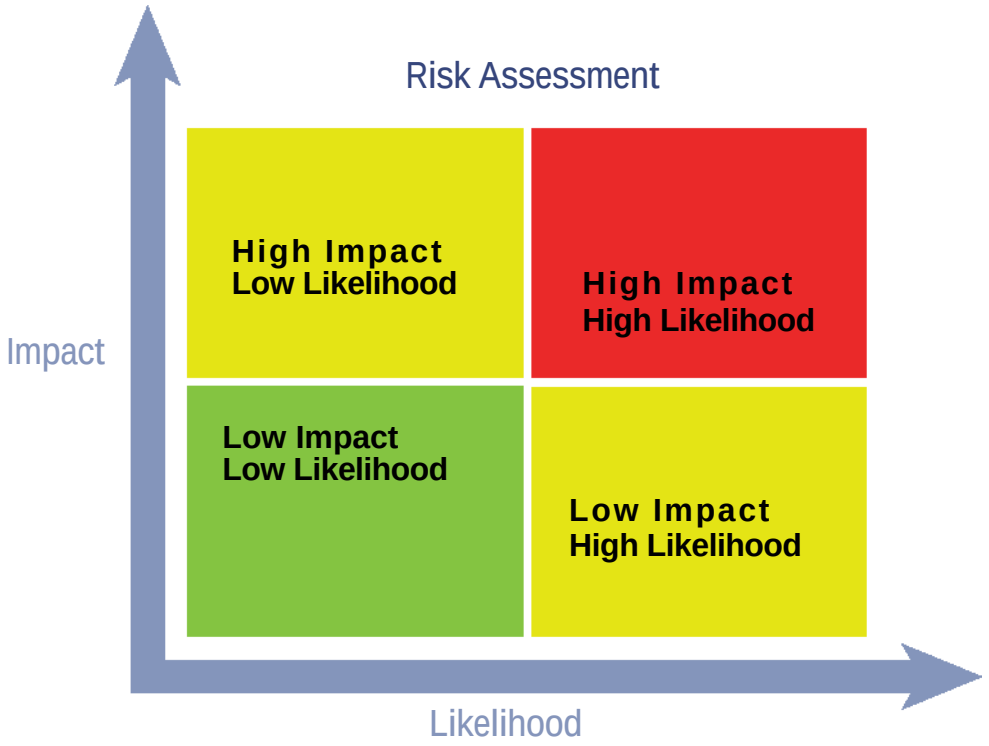
Every action or activity comes with an inherent risk.

Once identified, risks can be assessed according to their potential **Impact** and **Likelihood** (i.e. their probability of occurrence) considering the current controls in effect. Sometimes these factors can be relatively simple to measure, such as the value of a lost building. Sometimes evaluating risk can be very subjective.

RISK ASSESSMENT = IMPACT x LIKELIHOOD

Obviously, a prudent risk management plan concentrates on potential events which have both a high Impact and a high Likelihood of occurrence.

For purposes of our discussion, when we discuss a particular risk, we will acknowledge and consider existing controls.



Impact and Materiality

The impact and materiality of an event is determined according to the impact for the duration of the event or 36 months:

UW-Parkside Materiality

Materiality Area	Range of Metrics/Measures	Actual Figures	Low	Medium	High	Extreme	System Wide
Financial	**Biennial Reduction in Total Revenue:** Incorporates change in state support, tuition and fees, gifts, grants and contracts, endowments, and other income. Accounts for increases/decreases in expenses such as operating, debt, and loss. **Related Accountability Report Measure 5-1: Revenue**	2008-2009 total budget from redbook	Less than 1%	1-3%	3-7%	>7%	7%
	Parkside	$TBD	Less than $_____	Between_ and _M	between _M and __M	between __ M and __M	greater than __M
Students	**Annual Reduction in New Freshman Applications:** Incorporates change as influenced by factors such as high school graduate demographics, diversity/ equity, safety, and learning opportunity array.	Completed applications Fall 2008	<3%	3-6%	6-10%	>20%	>20%
	Parkside	TBD	reduction of less than ___	reduction of between ___ and ___	reduction between ___ and __	reduction of between __ and ___	greater than a ___ reduction
	Annual Reduction in Total Student Enrollment: Incorporates change as influenced by factors such as academic reputation, financial aid availability, program array, and faculty/staff resources.	2008 enrollment	flat	0-3% reduction	3-6% reduction	Greater than 6%	Greater then 3 percent system wide
	Parkside	TBD	flat	reduction of up to ___	reduction of ___ to ___	reduction of ___ to ___	Greater than ___
	Annual Percent Change in Six-Year Graduation Rate: Incorporates change as influenced by financial aid, student support services, and course availability. **Related Accountability Report Measure 2-4: Six-Year Graduation Rate**	2002 figures	>0.5%	0.5%-0%	0%-(0.5)%	>(0.5)%	
	Parkside	TBD%	greater than 60%	between 59.5 and 60%	between 59 and 59.5%	less than 59%	

Likelihood

There are four rating classifications based on the Likelihood that an event will occur over the course of the next 36 month period taking into consideration the current controls:

1 = Low – Possible but unlikely to occur; unlikely (less than 10%).

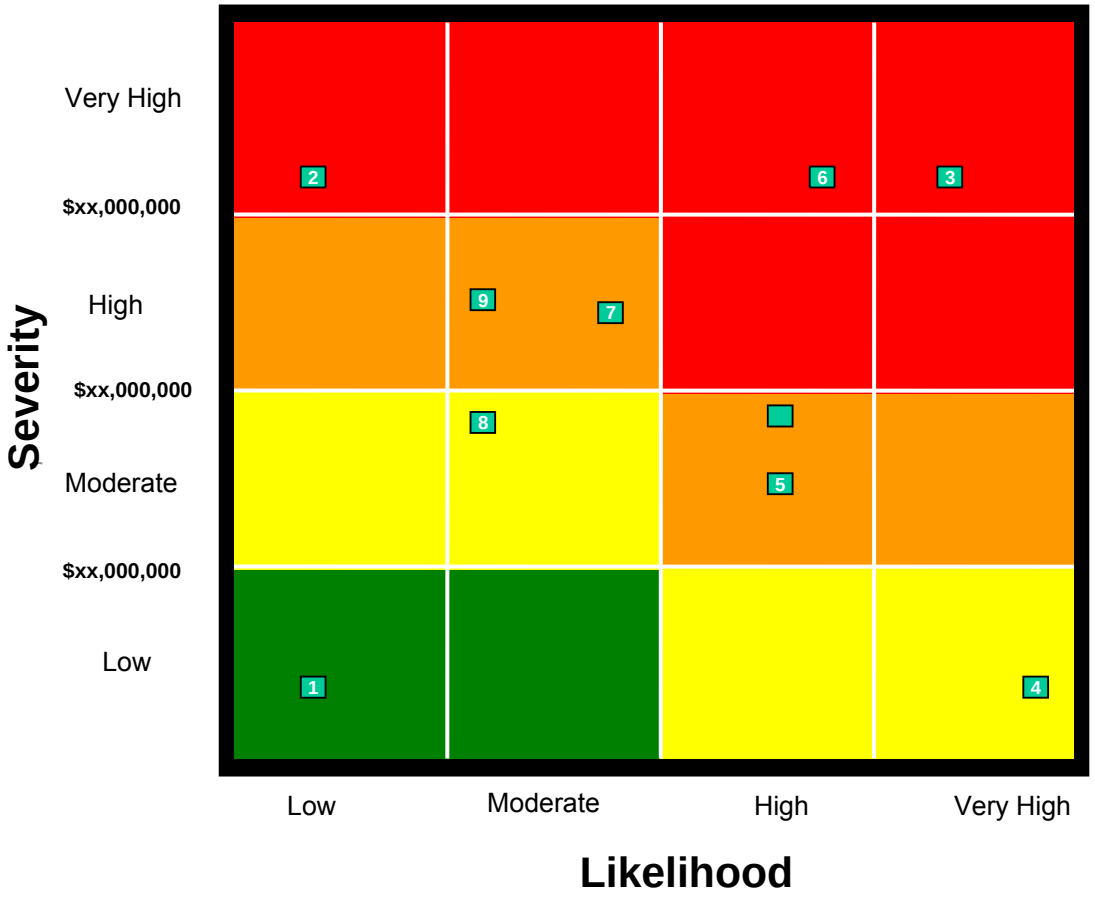
2 = Moderate – Moderate risk of occurrence; possible (between 10-50%)

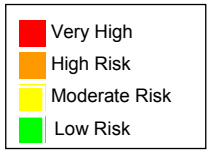
3 = High – Likely to occur; probably (between 50-75%)

4 = Very High – Very likely to occur in immediate future; (greater than 75% chance)

Risk Map (sample)

Once we're able to determine the likelihood that a potential event will occur and estimate its impact, the event can be plotted on the risk map. Threats with the highest potential risk (those appearing in the red and orange areas) are then assessed and evaluated as to the effectiveness of risk controls already in place. Threats that fall into the yellow and green categories ("medium" and "low" risk) will be submitted back to the management team to be addressed as part of normal operating procedures.





LEGEND

1 Fire at remote warehouse
2 Tornado
3 Fire on Campus
4 Academic Fraud - Scandal
5 Major travel accident
6 IT system failure due to lack of IT infrastructure control
7 Graduate program competition
8 Loss of loan funding
9 Pandemic

Risk Control Effectiveness

The next step is to evaluate the effectiveness of risk controls already in place. This by necessity is a subjective determination, using a four-tiered scale:

4 - Strong Controls
3 - Moderate Controls
2 - Limited Controls
1 - Weak Controls or No Controls

These controls can take a variety of forms. For example:

- **Rule-based** -- through policies, processes, controls, or performance standards.
- **Management control** -- where responsibility for control is assigned to a specific person or function within the organization.
- **Compliance-based** – a rule-based or management control where adherence is verified as part of a mandatory reporting process.
- **Physical controls** – using barriers or mechanical and/or computer controls to manage access.
- **Risk culture** – the tone set by the management of the organization about the importance of managing risk.

Risk Retention, Risk Mitigation, and Risk Ownership

Following risk analysis (Top-Down & Bottom-Up Workshops), Risks are placed in one of two categories – Risk Retention or Risk Mitigation: Risk retention simply means that a risk is accepted at this time and current controls are retained, maintained, and monitored. If a risk or threat is unacceptable and cannot be placed in risk retention, additional mitigation activities are developed. The risks are prioritized and programs, processes, or physical investments are identified that will control an event's impact and/or likelihood to a level which brings it into risk retention. Techniques may include finding a way to avoid the risk, transferring a risk through mechanisms such as insurance or outsourcing, or employing one or more of the risk controls previously mentioned.

Risk Ownership:

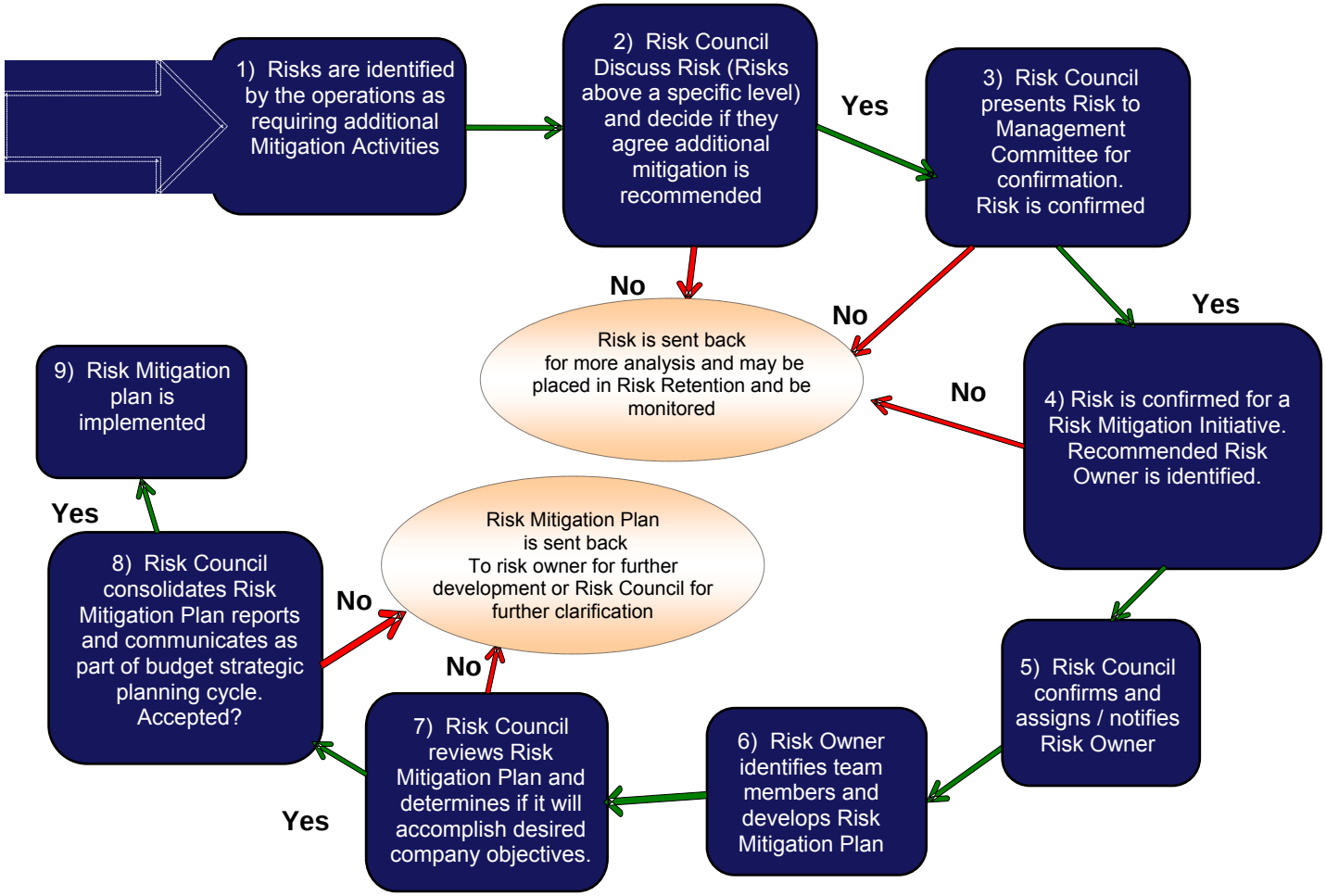
For risks identified as requiring risk mitigation activities to bring them into risk retention, a risk owner is identified.

The risk owner is the individual who will take the lead in developing the Mitigation Activity Plan(s). Typically, the risk owner will operate with direct support from the Risk Council and the business unit/senior management and will be able to call on others with specialized skills throughout the organization.

In addition to this lead role in the development and execution of the Mitigation Activity Plan(s), the risk owner will be responsible for communicating progress to the Risk Council and senior management.

ERM Risk Mitigation Process (recommended)

The following table shows the process through which an identified risk would follow once it is selected for Risk Mitigation Activities:



Glossary

Annual Risk Report	A document compiled by the Risk Council which consolidates ERM analysis, Recommendations, Mitigation Plans and their associated budgets for the entire organization. The Annual Risk Report is presented to the Executive Committee.
Risk Profile	A comprehensive view of the risks faced by the organization.
Central functions	Departments and central services that support and affect the business operations of the organization.
Enterprise Risk Management (ERM)	The University of Wisconsin System's comprehensive program designed to proactively and continuously identify and manage real and potential threats and opportunities that may impact our business.
Impact	Estimated financial cost that would be realized if a risk event were to occur. It is determined using the impact on revenue over a 36 month period.
Likelihood	The probability that a risk will occur.
Management Control	How well the organization is presently controlling/mitigating an identified risk. (Measured from "weak" to "strong".)
Materiality	Specific reference point used to categorize the magnitude of the Impact of a Risk. From Low to Very High/Extreme.
Materiality Levels	The thresholds that the organizatino uses to ascertain the Materiality of a Risk at the Enterprise and individual entity levels.
Mitigation Plan	A strategy for Risk Mitigation and its associated budget. If an identified Risk is not within Risk Retention, then further mitigation is planned.
Opportunity	A chance for advancement or progress.
Risk	A potential event with an undesirable/negative outcome, including the potential failure to capitalize on an Opportunity.
Risk Assessment	The process of identifying and analyzing risk.
Risk Category	Distinct classes of risks that allow Risk to be compared and analyzed.
ERM Risk Map	Graphical representation of the potential Impact and Likelihood that a Risk could present to, considering the Management Controls currently in place.
Risk Mitigation	A program, process, or physical investment which is intended to control or reduce a Risk's Impact or Likelihood.
Risk Owner	The Risk Owner is the individual identified to lead the development and implementation of the Risk Mitigation plan.
Risk Retention	If an identified Risk is within Risk Retention, then current controls are retained, maintained, and the identified Risk is monitored.
Threat	Something with the potential to cause damage, injury, or loss.