# Enterprise Risk Management Program Plan

May 2024

## Background

Risk is defined as uncertainty of outcomes, whether positive opportunity or negative threats, of actions and events[1]. Enterprise risk management is a holistic approach to managing risks; risks which can impact the successful execution of the university's mission and objectives.

The goal of the UCF enterprise risk management (ERM) program is to provide a systematic approach to identify and manage various types of risk, regardless of the origin. Risks can include those affecting the whole of higher education, risks specific to the UCF, or risks related to certain units and processes.

A robust ERM program will benefit UCF by:

- ✓ Better aligning UCF's strategy and objectives to its risk appetite: UCF has a mission and vision that provide the basis for decision-making. Strategy and objectives are developed to support the university mission and vision, the development and execution of which come with risks. ERM establishes a framework for effective decision-making regarding pursuit of strategies, initiatives, and programs including a mechanism to discuss when strategies are not aligned with the university's mission and vision.
- ✓ Identifying and managing risk enterprise-wide: The university is faced with a myriad of risks. Sometimes the impacts of those risks are localized to one area, but more often the impacts are felt across various departments. It is important to consider a risk from an enterprise perspective to understand how actions taken can affect other departments and partners. An ERM program provides the vehicle to identify, discuss, and manage risks at an entity level to ensure actions taken represent the best option for the university.
- ✓ Improving resource deployment: UCF, as is the case with many other entities, has finite resources and innumerable needs. Every unmet need represents a risk. The university must have a way to prioritize which risks should be addressed with the set number of resources available. ERM provides key information to focus university resources on critical risks with the potential for the most substantial impact. Additionally, ERM creates a mechanism to escalate risks when broader management and resources are needed.
- ✓ Enhancing resilience: The landscape of higher education continues to evolve and change. New opportunities and challenges are identified almost daily. The university's continued viability is contingent on its ability to anticipate and respond to change. An effective ERM program helps identify factors that represent not just risk, but change, and how that change could impact performance and necessitate a shift in strategy.

[1] Her Majesty's Treasury. Government and Finance Function. *UK Orange Book*, 2020. https://www.gov.uk/government/publications/orange-book

*Approved by the UCF Board of Trustees – June 24, 2024*

The university will take a phased approach to ERM implementation.

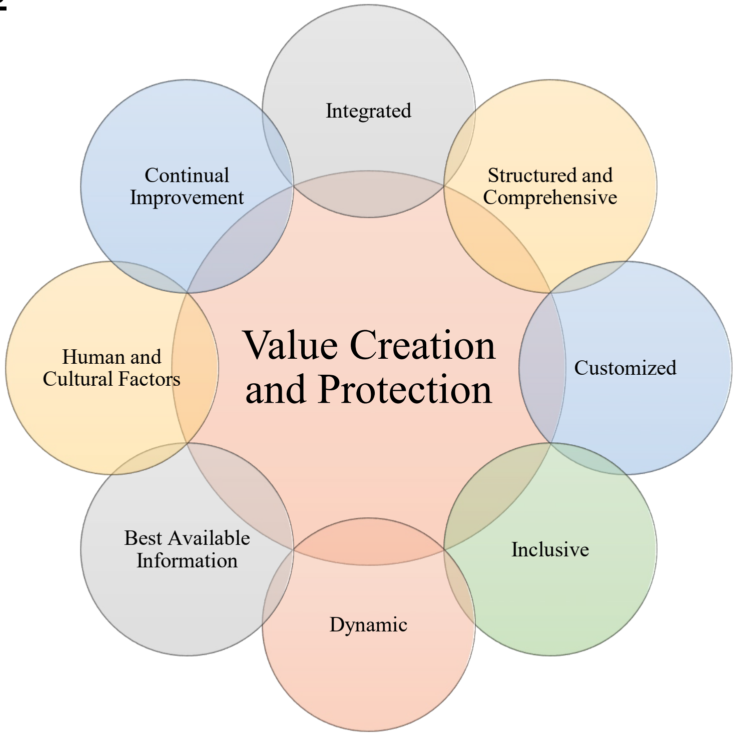
| |
|---|
| ***Phase 1: Targeted risk assessment and education*** |
| • Risk tabletop with university leadership |
| • Education of university leadership |
| • Risk assessment of key initiatives / topics |
| ***Phase 2: Program foundation*** |
| • Education of university units and offices |
| • Articulation of university risk appetite |
| • Implementation of risk governance structure |
| • Initial risk identification of university-wide risks |
| • Risk assessment of key initiatives and topics |
| ***Phase 3: Full program implementation*** |
| • Roll-out of ERM program |
| • Continued education of university community |
| • Evaluation of program effectiveness |

The sections below outline the university's ERM program including the risk management standard that will serve as the basis for the program and the process used to identify, analyze, and evaluate risks.

## Risk Management Standard: ISO 31000

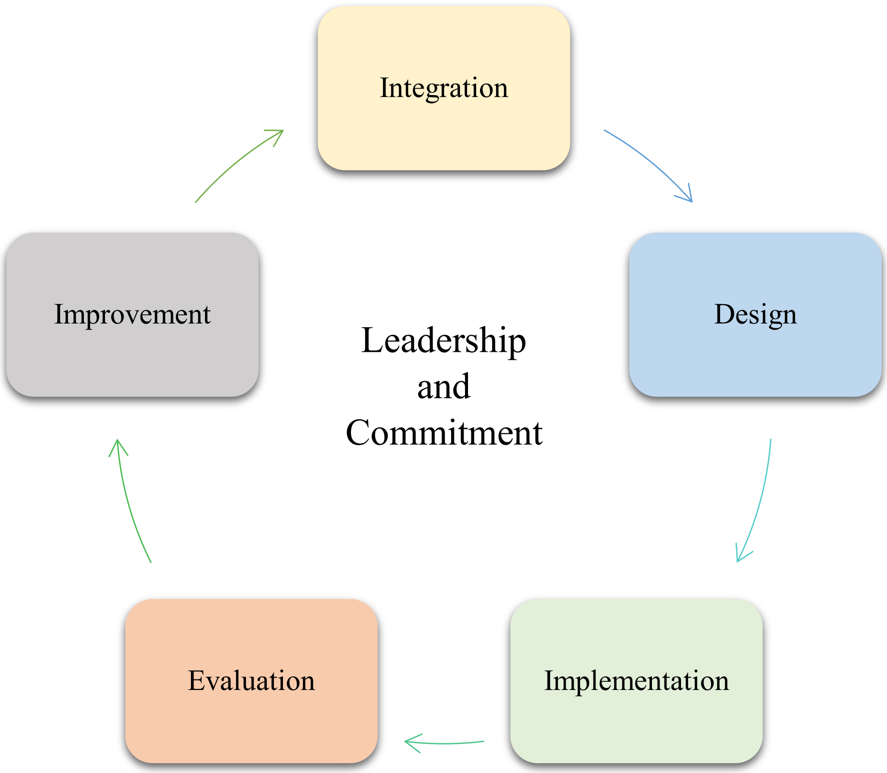
ISO 31000 is the only international standard on the practice of risk management. The best practice guidelines provide principles, a framework, and a process for managing risk, which it defines as "the effect of uncertainty on objectives". The standard is flexible and can be customized to any organization, including public entities and institutions of higher education. It can be applied to any activity and decision-making at any level of the organization. Using ISO 31000 can help increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment. The standard creates a foundation to implement, maintain, and continually improve the enterprise risk management of an organization. The three tenets of the standard are pictured and described below.

## ***Tenet 1: Principles***


Integrated
Structured and Comprehensive
Continual Improvement
Value Creation and Protection
Human and Cultural Factors
Customized
Best Available Information
Inclusive
Dynamic

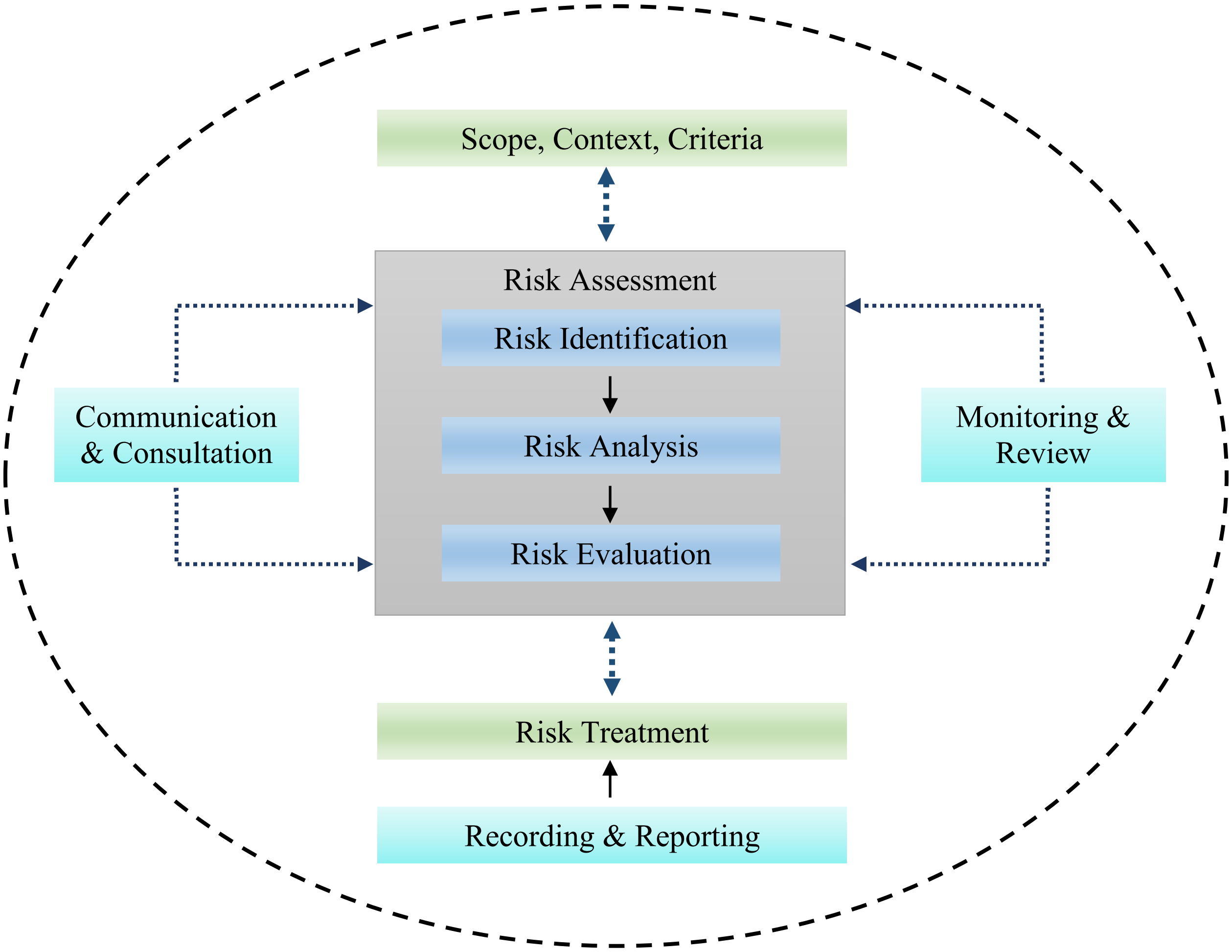
At its core, the purpose of ERM is to create and protect value of an organization. The principles serve as the basis for managing risk in a way that supports ERM's purpose. The eight principles outline important factors that should be incorporated when designing, planning, and implementing an effective ERM program. While each principle is important, having ERM embedded in the university's decision-making culture as well as establishing a program that can respond to risks as they emerge, change, or disappear are essential. The design and implementation of UCF's ERM program will be based on these principles.

## ***Tenet 2: Framework***



The framework provides guidance on implementing a value-creating program. One of the central elements of the framework is leadership and commitment. The UCF Board of Trustees and UCF leadership will be responsible for establishing the campus tone for ERM. The ERM program will align risk appetite to the university's objectives, strategies, and culture. To ensure the program is robust, it will be designed to factor internal and external aspects, establish and articulate roles and responsibilities, and integrate ERM into university activities, functions, and decision-making. The framework will be used to clearly define the decision-making process, communication expectations, and program objectives. UCF's ERM program will be continually monitored for improvement opportunities and modified as needed. Periodically, the ERM program will be evaluated for its effectiveness.

***Tenet 3: Process***



The process outlines the systematic tactical steps to implementing an ERM program. The process will engage multiple stakeholders across the organization to ensure different areas of expertise and risk are represented. The success of the ERM program will depend on input from various university members, and it will be important for each person to clearly understand the objectives, expectations, and value of the process. One of the key components of the risk process is to identify and implement the appropriate risk treatment strategy. Continually monitoring process outputs and communicating with leadership are essential fundamentals of the ERM process.

## Enterprise Risk Assessment Process

While the guidelines outline principles and a framework, the primary focus of the remainder of this document is on governance and process. The risk assessment process has three key steps: risk identification, risk analysis, and risk evaluation. Each step of the risk assessment process is outlined below including the governance structure to facilitate the risk assessment process.

## ***Governance***

As indicated in the framework overview, it is important to define the roles and responsibilities associated with ERM. While the role of managing risk is everyone's responsibility, certain functions will serve specific program oversight and facilitation functions.

| Role | Responsibilities |
|---|---|
| **Board of Trustees (Board)** | • Provide oversight of university's risks by understanding leadership's approach to managing risk including risk culture, current processes, and effectiveness of identifying and mitigating the most significant enterprise-wide risk exposures<br>• Provide oversight of the university's risk appetite and tolerance to be considered when approving strategy, making decisions, and managing relationships<br>• Set the tone for ERM and risk decision-making including fostering a culture of risk awareness |
| **Board of Trustees Audit & Compliance Committee** | • Oversee the university's ERM program<br>• Assist the Board in fulfilling its responsibility to oversee the university's management of risk<br>• Obtain an annual update on the university's enterprise risk management program and risk assessment process<br>• Update the Board on critical risks and risk-related considerations |
| **President and President's Cabinet** | • Accountable to the Board to manage the university's risks including those with the most significant risk exposure<br>• Set university risk appetite and tolerance<br>• Report to the Board on enterprise risk topics<br>• Develop university strategy and ensure strategy's alignment with mission, vision, and risk appetite<br>• Review, validate, and / or revise the university's risk priorities<br>• Review proposed mitigation plans associated with certain enterprise-level risks and ensure plans align with university's strategy, objectives, and budgetary resources<br>• Establish "tone" for the university regarding ERM by fostering a culture of risk awareness and actively supporting the development and implementation of the ERM program<br>• Allocate resources to manage and mitigate risks |
| **`Risk Champions** | • Serve as an ERM liaison within their respective organization which includes supporting department / unit in (1) understanding ERM and risk, (2) risk-aware decision-making, (3) identifying and analyzing risks<br>• Review landscape to identify emerging or changing risks<br>• Support Office of Enterprise Risk and Insurance in prioritization of risks |

| | |
|---|---|
| | • Make recommendations on mitigation, where applicable<br>• Identify risk owners for key risk areas<br>• Support university-wide risk management including addressing functional, cultural, and departmental barriers to managing risks |
| **Office of Enterprise Risk and Insurance** | • Accountable to the President's Cabinet to prioritize identified risks<br>• Advise Board, President, and university on risk management topics<br>• Facilitate ERM program implementation and execution including providing ongoing oversight and management<br>• Maintain university risk universe and coordinate risk reporting<br>• Develop and maintain risk assessment procedures, tools, and documents<br>• Provide support for risk aware decision-making |
| **Risk Owners** | • Manage and mitigate risks<br>• Partner with the Office of Enterprise Risk and Insurance to assess and report risks<br>• Embed risk management thinking into decision making |

## ***Risk Identification***

The first step of the risk assessment process is risk identification. Risk identification involves scanning the internal and external environment for events, decisions, or actions that may impact the university's objectives. This process will occur by conducting one-on-one interviews, facilitated risk workshops, and surveying across campus. During risk discussions, the Office of Enterprise Risk and Insurance will seek to gather information regarding key business processes, legal and regulatory requirements, key suppliers and contracts, technology systems, major initiatives, and challenges faced by the unit. The Office of Enterprise Risk and Insurance will summarize the output and define the risks identified from the discussion; internal risk identification will be supplemented with risks from higher education and other sources as applicable. In conjunction with risk champions, risks will be appropriately categorized. Risks will be organized based on the categories outlined below. The categories will be further divided into sub-groups based on the specific nature of the risk.

The Office of Enterprise Risk and Insurance will provide tools to the university community to identify risks which can be used to evaluate changes to operations, new opportunities and partnerships, and / or new laws or requirements. Providing tools along with education will support embedding risk thinking into university decision-making. The formal risk identification process facilitated by the Office of Enterprise Risk and Insurance will occur every three years.

Categories of Risk

- **Compliance / Legal / Regulatory** – Risks related to adherence to federal and state laws and regulations, local municipal laws, case law, accreditation standards, university policies and procedures, and contractual obligations, including contractual agreements, employment contracts, and collective bargaining agreements.

- **Operational** – Risks related to people, processes, and technology systems including efficient and effective use of university resources.
- **Financial** – Risks related to the university's financial position and resources including tuition, government support, gifts, research funding, endowment, budgeting, accounting and reporting, investments, credit rating, fraud, cash management, long-term debt, etc.
- **Hazard / Safety** – Risks related to injury, damage, or health and safety of the campus population, including impacts caused by accidental or unintentional acts, errors or omissions, or external events such as natural disasters.
- **Strategic** – Risks related to achievement of UCF's strategy including development and execution of business plans and initiatives, change and disruption management, competition, adaptation, innovation etc.

Reputational risk is inherent in all activities and present in each risk category. Therefore, UCF's reputation will be evaluated for each risk as opposed to a defined risk category.

## ***Risk Analysis***

Once risks have been identified, the potential impacts to the university need to be considered. The risk analysis step will segregate risks into enterprise-level and unit-level risks and prioritize based on potential exposure to the university. To prioritize the various risks and thus the areas of focus, the impact, likelihood, velocity, and complexity of the enterprise risks will be defined. A consistent scale and formula will be used to comparably analyze and develop a risk score (see below). A summary of risks identified will be reviewed with each dean and vice president. The full set of risks will be shared with University Audit to support risk-based audit planning.

| **Inherent Risk Ranking** | **High (5)** | **Medium (3)** | **Low (1)** |
|---|---|---|---|
| Reputational Impact (25%) | Potential for extensive media coverage or impact to UCF brand; failure to meet stakeholder expectations and loss of stakeholder trust; community engagement and participation impaired | Potential for significant media coverage or impact to UCF brand; inability to meet stakeholder expectations; community engagement and participation affected | Potential for little to no media coverage or impact to UCF brand; stakeholder expectations met or exceeded; community engagement and participation remain high |
| Financial Impact (20%) | Significant portion of federal funding, state funding, endowments, or auxiliary revenue at risk; research grant funding substantially impacted; inefficient and excessive costs with minimal to no positive return | Some portion of federal funding, state funding, endowments, or auxiliary revenue in jeopardy; research grant funding potentially impacted; inefficient cost management; significant additional costs to university | Ability to maintain level of federal funding, state funding, endowments, and auxiliary revenue to support university operations; research grant funding sustained; costs effectively managed; no additional costs to university |

| | | | |
|---|---|---|---|
| Operational Impact (20%) | Potential for major disruption or impairment to any of the following: academic activities, research activities, core or support activities, athletics, ability to meet student needs; expected to occur for sustained duration with long-term effects | Potential for moderate disruption to any of the following: academic activities, research activities, core or support activities, athletics, ability to meet student needs; disruption may occur for sustained period | Negligible to minor delay or disruption to any of the following: academic activities, research activities, core or support activities, athletics, ability to meet student needs |
| Complexity (10%) | Little to no understanding of topic, topic extremely dynamic or yet to be fully defined; significant gaps exist in resources to address, highly inter-connected with other risks, initiatives, and / or processes | Topic not fully understood and some variability present; limited resources exist to properly address; some interdependencies identified with plans for management in place. | Well-defined and understood topic; resources available to address; interdependencies limited and / or well-managed |
| Likelihood (10%) | High probability of occurrence in next five years and / or occurs quite often. | As likely to occur as not in the next five years and / or occurs sometimes | Low probability of occurrence in the next five years and / or occurs in rare occasions |
| Velocity (15%) | Impact materializes in days, weeks, or months | Impact materializes in one to three years | Impact materializes in three years or greater |

Stakeholders widely defined as any of the following groups: students, parents, donors, regulators, legislators, Board of Governors, partnership associates, and the surrounding community.

**Risk Score** = Risk ranking weighted average

## ***Risk Evaluation***

The last step of the risk assessment process is to evaluate each risk in support of decision making. Risk evaluation leverages output of risk analysis to determine the appropriate next step to best protect the university. Next steps could include:

- ✓ Further analysis of the risk,
- ✓ Better understanding of risk treatment options,
- ✓ No additional steps based on the potential exposure, existing management, and available mitigation options.

For unit-level topics, the Office of Enterprise Risk and Insurance will provide a self-assessment tool to guide the decision-making process for each of the unit's risks. In determining additional actions, the university's mission, goals, objectives, and risk appetite and tolerance must be considered.

It is the responsibility of department leaders to escalate, as needed, any topic which would represent an enterprise risk either due to change in exposure or further evaluation. Risks should be escalated to the risk champion for their respective area. For risks identified as enterprise, the Office of Enterprise Risk and Insurance will work with risk owners and appropriate parties to understand the various drivers, existing risk mitigation and controls, and mitigation gaps, if any. If it is determined efforts are insufficient, the risk owner in conjunction with the Office of Enterprise Risk and Insurance, will evaluate if objectives should be reconsidered, further analysis conducted, or additional controls and plans implemented.

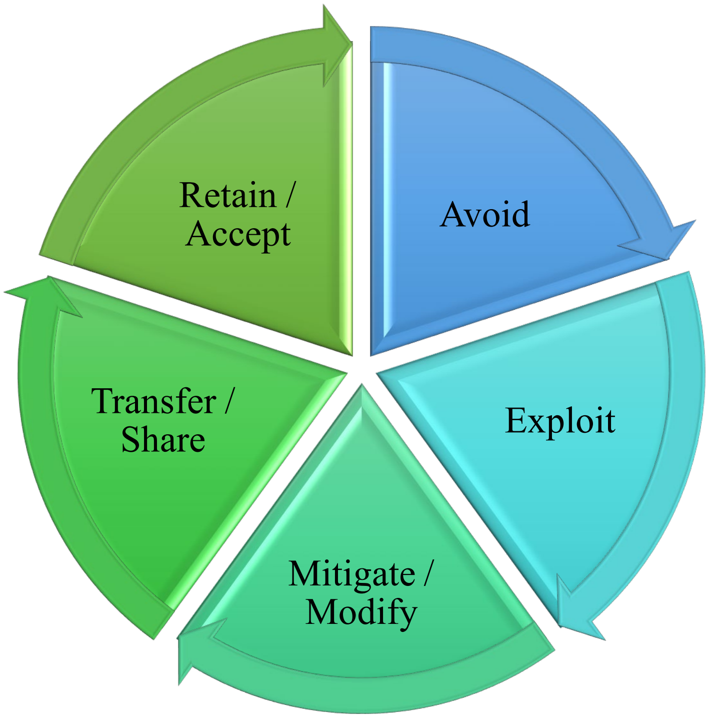
*Approved by the UCF Board of Trustees – June 24, 2024*

# Enterprise Risk Treatment

Each step of the assessment process leads to determining how to best treat and manage risk. The purpose of risk treatment is to select and implement options for addressing risk. The process of risk treatment is iterative and includes:

1) Selecting treatment options,
2) Planning and implementing options,
3) Assessing effectiveness of treatment,
4) Deciding whether remaining risk is acceptable, and
5) Taking additional action if needed.

**Risk Treatment Strategies**



A combination of treatment options may be most appropriate. Selecting risk treatment option(s) should involve balancing the potential benefits versus costs, effort, or disadvantages of treatment option. If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review. For unit-level topics, the Office of Enterprise Risk and Insurance will provide a treatment and response plan template for units to collect key elements of treatment plans including responsible parties and actions. For risks identified as enterprise, risk owners, with support from the Office of Enterprise Risk and Insurance, will develop a treatment and response plan including a monitoring and communication strategy.

Based on the score of the risk determined during the risk analysis step, the following evaluation, management response, communication, and monitoring are recommended:

| Risk Score | Response for Enterprise Risks |
|---|---|
| **1.0 – 2.3** | ○ Risk evaluation conducted at the unit level with support as needed from Office Enterprise Risk and Insurance<br>○ Treatment and response plan developed at the unit level<br>○ Periodic review and monitoring by appropriate university leadership<br>○ Communication of risk and plan(s) to appropriate university leader |
| **2.4 – 3.7** | ○ Risk evaluation conducted at the unit level with support as needed from Office of Enterprise Risk and Insurance<br>○ Treatment and response plan developed at the unit level<br>○ Continuous monitoring and periodic review by appropriate university leadership<br>○ Communication of risk and plan(s) to appropriate university leader and President, as needed |
| **3.8 – 5.0** | ○ Risk evaluation conducted by Office of Enterprise Risk and Insurance to support risk treatment plan development and resource allocation decisions<br>○ Development of treatment plan in 6 – 12-month timeframe<br>○ Continuous review by university leadership<br>○ Communication of risk and plan(s) to appropriate university leader, President, and Board, as needed |

## Enterprise Risk Management Communication

To support the Audit and Compliance Committee's oversight role, the Office of Enterprise Risk and Insurance will provide an annual update on the current state of the ERM program. Additionally, the Office of Enterprise Risk and Insurance will partner with the Board Relations Office to drive Board and Committee agenda items, as needed, based on topics identified during the assessment process. Annually the President and Cabinet will also receive an update. Department leaders will be responsible for providing updates to the President and respective Cabinet members on enterprise and / or unit risks as needed.