Enterprise Risk Management (ERM):

Implementing a Risk Assessment

March 2022

Judy Burns, Enterprise Risk Officer
UT System Office of Finance and Administration

THE UNIVERSITY OF TENNESSEE

OVERVIEW

Enterprise Risk Management

Enterprise Risk Management (ERM) is framework for managing risk. ERM’s goal is to improve an organization’s performance toward the achievement of its goals and objectives. In this context, “risk” is an umbrella term for uncertainties that may either positively (opportunities) or negatively (threats) impact goals and objectives.

Risk is managed by an organization’s leaders. They can use the information gained through the implementation of an ERM framework in strategy-setting, planning, decision-making, and resource allocation.

ERM frameworks can be applied to the entire organization (e.g., the UT System) and/or its components (e.g., a campus/institute, a college, or a department). The framework can also be used when considering a new initiative (e.g., acquiring a new undergraduate campus) or the management of a functional area (e.g., HR).

Implementing an ERM framework can provide leaders with:

- A top-down holistic perspective of risk across the entire organization, leading to better decisions on priority setting and resource allocation,
- A deeper understanding of the uncertainties facing the organization, its ability to address those uncertainties, and the alternatives for responding, and
- A means of assuring the organization’s stakeholders that risk is appropriately addressed.

When used throughout an organization, an ERM framework provides a consistent methodology and language for communicating about and responding to risk as it relates to the achievement of mission, goals, and objectives.

State of Tennessee Requirements

The impetus for the University of Tennessee’s (UT) ERM initiative is guidance issued by the Tennessee Department of Finance and Administration (TN F&A) on how to comply with the Tennessee Financial Integrity Act of 1983 (TFIA). Amended over the decades, TFIA requires state agencies to assess risks and internal controls.

TN F&A’s most recent guidance (October 2016) requires agencies’ risk assessments to align with the Committee of Sponsoring Organizations’ (COSO) framework on ERM, *Enterprise Risk Management—Aligning Risk with Strategy and Performance* (2017). (COSO is an initiative involving five professional associations—American Accounting Association, American Institute of CPAs, Financial Executives International, Institute of Management Accountants, and The Institute of Internal Auditors. Formed in 1985 to address fraudulent financial reporting, COSO’s mission has expanded to now provide leadership on methods to improve organizational performance and governance.)

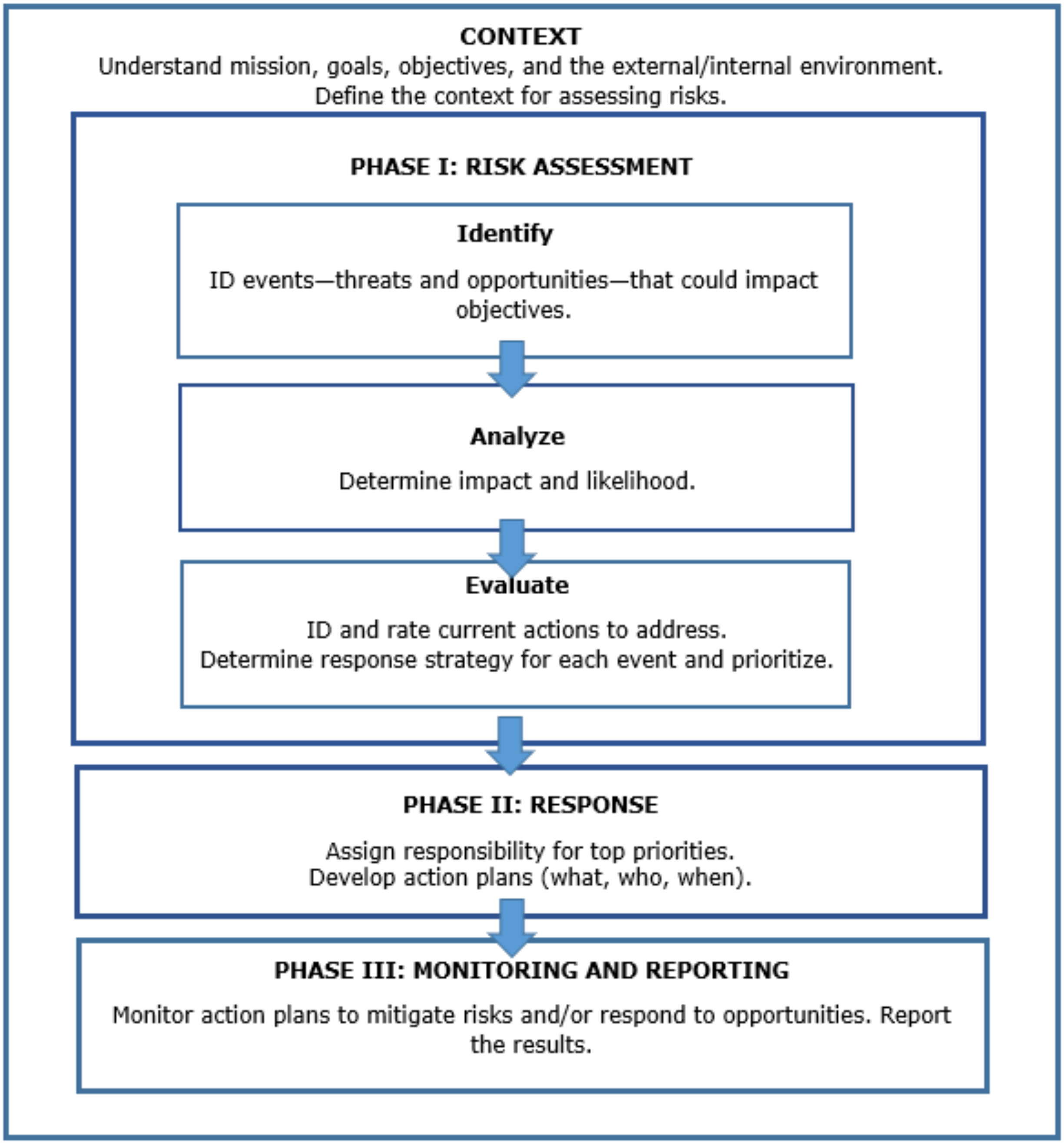
Purpose

ERM at UT will initially involve three phases: Phase I Risk Assessment, Phase II Risk Response, and Phase III Monitoring and Reporting Results.

The purpose of this document is to provide guidance for implementing the Phase I Risk Assessment: identifying, analyzing, and evaluating risks (positive and negative) to goals and objectives.

The following graphic presents an overview of The University of Tennessee's ERM framework. Appendix 3 contains a glossary of key ERM terms.

ENTERPRISE RISK MANAGEMENT AT UT



CONTEXT

Understand mission, goals, objectives, and the external/internal environment.
Define the context for assessing risks.

PHASE I: RISK ASSESSMENT

Identify

ID events—threats and opportunities—that could impact objectives.

Analyze

Determine impact and likelihood.

Evaluate

ID and rate current actions to address.
Determine response strategy for each event and prioritize.

PHASE II: RESPONSE

Assign responsibility for top priorities.
Develop action plans (what, who, when).

PHASE III: MONITORING AND REPORTING

Monitor action plans to mitigate risks and/or respond to opportunities. Report the results.

COMMUNICATION AND EXAMINATION OF ERM PROCESS

Share information regarding risk management activities throughout the organization.

Communicate risk management activities to internal and external stakeholders.

Periodic examination, assessment, and revision of ERM process.

ENTERPRISE RISK MANAGEMENT

Overview of Phase I: Risk Assessment

A risk assessment consists of three principal activities: 1) identifying risks, 2) analyzing risks, and 3) evaluating risks to determine how to respond. Risks are uncertainties that could *either* threaten the achievement of goals and objectives or present opportunities.

Suggested steps for each activity are detailed below.

Activity 1: IDENTIFY risks

Step 1: Brainstorm a list of risks (threats and opportunities)

Step 2: Identify key risks (the top 3-6)

Step 3: Write risk statements

Activity 2: ANALYZE the most significant risks by determining magnitude of impact and likelihood of occurrence.

Step 1: Determine magnitude of impact (high, medium, low) of the key risks

Step 2: Determine likelihood each key risk will occur within the next 2-3 years (high, medium, low)

Step 3: Provide a brief explanation or reasons for the selected ratings.

Activity 3: EVALUATE to determine the response strategy for top priority risks

Step 1: Identify any current actions at the University related to each of the key risks and rate the adequacy of those actions (sufficient or insufficient)

Step 2: Choose a response strategy for each risk (threats and opportunities)

Step 3: Recommend who (position and office) should be responsible for implementing the response for each top priority risk that requires action.

Activity 1: IDENTIFY

Objective: To identify and define potential events (threats and opportunities) that could affect the achievement of the University's goals and objectives.

Use the Excel workbook "ERM Activity 1_Identify Threats and Opportunities" to document the results of Steps 1 and 2.

Step 1: Brainstorm a list of potential events (threats and opportunities) that could affect the achievement of the University's goals and objectives.

Guidelines:

- Focus on events that could occur within the next 2-3 years.
- Generate as many ideas as possible; in the next step, you will prioritize and, later, refine.
- Consider:
  - Changes in the higher education environment (funding, public perception, stakeholder expectations, new approaches in teaching or research, new technologies, etc.).
  - Changes in the broader external environment (economic, regulatory, political, social, cultural, etc.).
  - Changes within the University of Tennessee (organizational changes, personnel changes, funding, new programs/activities, new technologies, new regulations, etc.).
- Discuss causes and effects of events whenever possible. Doing so will help with the next steps.

Appendix 1 contains a table listing some categories of events and corresponding descriptions that may stimulate your thinking.

Step 2: Identify the key threats and opportunities (top 3-6).

Guidelines:

- Reach consensus on the top risks.
- Rank order the risks, with #1 being the top priority.

Step 3: Write risk statements for the key threats and opportunities.

After you have identified the key risks (top three threats and top three opportunities) that may impact the achievement of objectives, the next step is to refine those thoughts by creating descriptive statements.

Crafting a structured statement ensures that you have thoroughly considered the event's effect on objectives and are able to communicate that idea clearly to others. It will also assist in determining appropriate responses to the events.

Following are some suggested structures.

The statement could take an "if-then" or "condition-effect" format:

- If <*negative or positive event that may happen*>, then <*negative or positive consequence on objective*> may result.
- <*Description of existing situation*> may lead to <*negative or positive consequence*>.

Examples of risk statements:

- If <*Congress approves a reduction in the federal facilities and administrative cost rate*>, then <*the cost of supporting current research projects could prevent UT from pursuing additional sponsored projects*>.
- <*The expansion of the Tennessee Reconnect program to allow adults to attend community colleges tuition free*> may result <*in a need to create new retention strategies for members of this population who enroll at UT*>.

Activity 2: ANALYZE

Objective: To determine the magnitude of the impact potential events (threats and opportunities) would have on the achievement of goals and objectives if they occurred and the likelihood the events will occur.

Use the Excel workbook "ERM Activity 2_Analyze Threats and Opportunities" to document the results of Steps 1 and 2.

Step 1: Determine the level of impact the key events would have on goals and objectives if they were to occur.

Appendix 2 contains specific types of impacts for each rating level that may help you determine a rating.

Table 1. Level of Impact

Rating	Description
High	The impact would preclude or highly impair (threats)/facilitate or significantly enhance (opportunities) the organization's ability to achieve goals or objectives.
Medium	The impact could significantly affect the organization's ability to achieve goals and objectives.
Low	The impact will not significantly affect the organization's ability to achieve one or more of its goals or objectives.

Step 2: Determine the likelihood the event will occur within the next 2-3 years.

Table 2. Likelihood of Occurrence

Rating	Description
High	The event is very likely or reasonably expected to occur.
Medium	The event is more likely to occur than unlikely.
Low	The event is unlikely to occur.

Step 3: Provide a brief explanation or reasons for choosing the selected impact and likelihood ratings.

Activity 3: EVALUATE

Objective: To determine how the University should respond to the top priority risks—threats or opportunities—identified.

Use the Excel workbook "ERM Activity 3_Evaluate Threats and Opportunities" to document the results of Steps 1 and 2.

Step 1: Identify any current actions/activities at the University related to any of the top threats and opportunities.

Using best judgement, determine whether the current actions/activities are adequate or inadequate for addressing the event. (Aim to evaluate the effectiveness of *each* action/activity.)

Step 2: Keeping in mind the ratings and the assessment of current activities, recommend a response strategy for each of the top threats and opportunities. Select from the strategies in Table 1 for threats or Table 2 for opportunities.

Table 1. Risk Response Strategies for Threats

Avoid: an informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk
Share: share the risk with other parties, including co-sourcing, outsourcing, or insurance
Mitigate: take action to reduce a risk's occurrence or the impact of its consequences if it does occur
Accept: an informed decision to tolerate a particular risk and take no additional action

Table 2. Risk Response Strategies for Opportunities

Ignore: an informed decision, based on currently available information, to decline to pursue a potential opportunity or consider it further
Share: partner, subcontract with, or acquire another party to pursue the opportunity or refer the opportunity to another party
Defer: postpone immediate action to monitor evolving circumstances surrounding the opportunity and/or to gain additional knowledge
Pursue**:** an informed decision, based on currently available information, to create an action plan to be involved in an activity or event that would increase the chances of achieving goals and objectives

Step 3: Recommend who (position/office) should be responsible for implementing the response strategy for each of the top priority risks (threats and opportunities).

Appendix 1

Event Categories*

Category	Description
Compliance	Changes in federal, state, or local laws and regulations, or University policy.
Financial	Physical assets or financial resources, such as: tuition government support, gifts, research funding, endowment, budget, accounting and reporting, investments, credit rating, fraud, cash management, insurance, audit, financial exigency plan, long-term debt, deferred maintenance
Hazard, Safety, or Legal Liability	Legal liability (negligence), injury, damage, or health and safety of the campus population or the environment, including impacts caused by accidental or unintentional acts, errors or omissions, and external events such as natural disasters.
Human Capital	Investing in, maintaining, and supporting a quality workforce, such as: recruitment, retention, morale, compensation and benefits, change management, workforce knowledge, skills, and abilities, employment practices
Operational	Management of day-to-day University programs, processes, activities, and facilities, and the effective, efficient, and prudent use of the University's resources.
Strategic	The University's ability to achieve its strategic goals and objectives, including competitive market risks, and risks related to mission, vision, values, strategic goals; diversity; academic quality; research; student experience; business model; market positioning; enrollment management; ethical conduct; accreditation

*Categories and definitions from the University of Vermont's "Guide to Risk Assessment and Response" (August 2012).

Appendix 2

Level of Impact	**Type of Impact**
Low	• Minor financial loss/gain, • Short-term local negative/favorable publicity, • No report/disclosure to regulator/third parties, • No or minor injuries, • Isolated staff morale problems/boost of morale, • Increase in turnover
Medium	• Significant financial loss/gain, • Short-term regional or national negative/favorable publicity, • Reportable incident to regulator/third party with remedial action required, • Injuries resulting in medical treatment, • Lawsuits, • Awards/recognition from local/regional bodies, • Widespread morale problems/boost of morale, • High turnover in certain areas/increase in employee retention
High	• Financial loss resulting in layoffs/discontinuation of services, • Significant financial increase, • Long-term regional/national/international negative/favorable publicity, • Reportable incidents to regulator/third party with penalties/suspensions/fines, • Class action lawsuits, • Awards/recognition from national or international bodies, • Widespread dissatisfaction with organization, • Majority of employees highly satisfied with organization, • High turnover of experienced staff and leadership positions/hiring of recognized leaders in their fields

Appendix 3

Key ERM Terms

Context: The area or circumstances around which risk management activities occur. The context for a risk assessment, for example, could be the entire organization, an organizational component, or an initiative.

Enterprise risk management (ERM): The capabilities and practices used to identify, assess, and respond to risk, the uncertainties (threats and opportunities) that may impact goals and objectives. ERM results in a top-down, holistic view of the organization's most significant threats and opportunities.

Environment, external: External environment in which the organization seeks to achieve its objectives, including cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environments, whether international, national, regional, or local; key drivers and trends; and relationships with, perceptions, and values of external stakeholders.

Environment, internal: Internal environment in which the organization seeks to achieve its objectives, which can include governance, organizational structure, policies, resource and knowledge capabilities, information systems and flows, decision-making processes, culture, form and extent of contractual relationships, and relationships with, perceptions, and values of internal stakeholders.

Event: Occurrence or change of a particular set of circumstances. Can be one or more occurrences, can have several causes, and can consist of something not happening.

Impact (consequence): The extent to which an event might positively or negatively affect the organization. Impact may fall into any of the following categories: financial, reputational, regulatory, health, safety, security, environmental, employee, stakeholder, or operational.

Likelihood: The chance that something will happen, expressed quantitatively, using the best judgement of responsible officials.

Responsible official (RO): Office or official with the accountability and authority to respond to a risk.

Risk: A potential event (an uncertainty)—either positive (opportunity) or negative (threat)—that may impact an organization's ability to achieve its goals and objectives.

Risk assessment: Overall process of identifying, analyzing, and evaluating risks (uncertainties) with the goals of assisting in strategy-setting, decision-making, and resource allocation; assuring stakeholders that risks are appropriately addressed; and improving outcomes in achieving goals and objectives.

Risk response: Process to respond to a risk, involving one or a combination of the following:

For negative risks (threats):

Avoid: An informed decision not to be involved in, or to withdraw from, an activity, in order not to be exposed to a particular risk.

Accept: An informed decision to tolerate a particular risk and take no additional action.

Mitigate/Reduce: Take actions designed to reduce a risk or its consequences. Usually requires an action plan to address.

Share/Transfer: Transfer risk, preferably contractually, to other parties, including insurance.

For positive risks (opportunities):

Ignore: An informed decision, based on currently available information, to decline to pursue a potential opportunity or consider it further.

Share: Partner, subcontract with, or acquire another party to pursue the opportunity or refer the opportunity to another party.

Defer: Postpone immediate action to monitor evolving circumstances surrounding the opportunity and/or to gain additional knowledge.

Pursue: An informed decision, based on currently available information, to create an action plan to be involved in an activity or event that would increase the chances of achieving goals and objectives

Risk response plan: Plan to implement chosen risk response. Action plans should include the following: tasks, position/persons assigned to tasks, timeframe for completion, and resource requirements. Response plans may be focused on mitigation of threats or pursuit of opportunities.

Risk statement: Structured statement of risk that describes the potential event and its impact on the achievement of goals and objectives. Whenever possible, the statement should also contain the cause or trigger for the event.