Enterprise Risk Management (ERM):
Developing Risk Responses

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.)

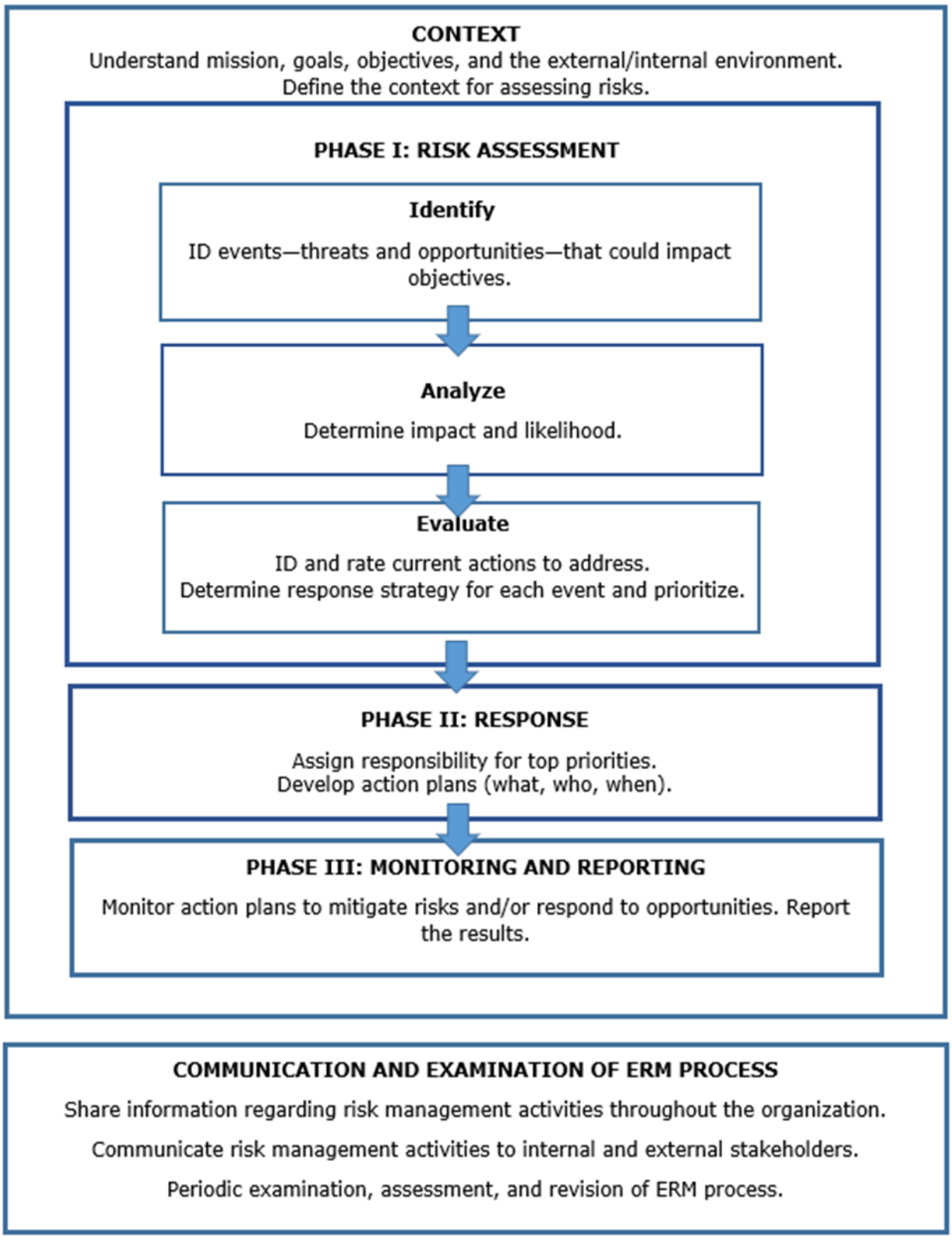
Purpose

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 the leaders who conducted the Phase I risk assessment with guidance for implementing Phase II: Risk Response. This phase consists of two key activities: assigning responsibility for responding to the top priority risks (threats and opportunities) and requesting documented action plans that outline the response activities from the responsible officials.

The following graphic presents an overview of The University of Tennessee's ERM process. Appendix 1 contains a glossary of key ERM terms.

ENTERPRISE RISK MANAGEMENT AT UT



ENTERPRISE RISK MANAGEMENT

Phase II: Risk Response

Realizing benefits from a risk assessment requires taking actions to respond to the top priority threats and opportunities. Responding requires the leaders who led the risk assessment to engage in two key activities: assigning responsibility and requesting action plans.

Suggested steps are below.

Activity 1: ASSIGN RESPONSIBILITY FOR RISK RESPONSES

Objective: To assign responsibility for leading the risk response to each top priority threat and opportunity to a specific position/office.

Step 1: Assign responsibility to the position/office that has the knowledge, skills, and abilities and scope of influence to address. (Keep in mind the response strategy previously identified for each threat or opportunity as the responsibilities are assigned. See the table in Appendix 2 for the strategies and their definitions.)

Step 2: Document to whom the individual threats and opportunities have been assigned.

Use the Excel workbook "ERM Activity Risk Response_Responsibilities" to document the assignment of responsibilities.

Step 3: Ensure the position/office assigned responsibility is informed of the assignment and briefed on the risk assessment that led to this responsibility.

Activity 2: REQUEST ACTION PLANS

Objective: To ensure that appropriate action plans are developed and implemented for responding to key threats and opportunities.

Step 1: Request from the responsible position/office a documented action plan for responding to the risk with the following elements:

- Actions
- Timeline
- Persons responsible
- Additional resources (funding, equipment, etc.)

Use the Excel workbook "ERM Activity Risk Response_Action Plans" as a template for action plans.

Step 2: Review action plans and provide any needed feedback or revisions.

Appendix 1
Key ERM Terms

Context, 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.

Context, 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.

Enterprise risk management (ERM): A structured process used to identify, assess, and respond to uncertainties that may impact goals and objectives. The process results in a top-down, holistic view of the most significant risks to an organization.

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 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) that may impact an organization's ability to achieve its goals and objectives.

Risk assessment: Overall process of identifying, analyzing, and evaluating risk with the goal of assisting in strategy-setting, decision-making, and resource allocation; assuring stakeholders that risks are appropriately addressed; and improving outcomes in

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

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.

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

Risk response plan: Plan to implement chosen risk response. Action plans must include: tasks, position/persons assigned to tasks, timeframe for completion, and resource requirements.

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

Appendix 2

Risk Response Strategies

Threats		Opportunities	
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	**Ignore**	An informed decision, based on currently available information, to decline to pursue a potential opportunity or consider it further
Share	Share the risk with other parties, including co-sourcing, outsourcing, or insurance	**Share**	Partner, subcontract with, or acquire another party to pursue the opportunity or refer the opportunity to another party
Mitigate	Take action to reduce a risk's occurrence or the impact of its consequences if it does occur	**Defer**	Postpone immediate action to monitor evolving circumstances surrounding the opportunity and/or to gain additional knowledge
Accept	An informed decision to tolerate a particular risk and take no additional action	**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