Enterprise Risk Management (ERM) Framework for
Western Washington University

DRAFT June 1, 2018 Rev 2
Table of Contents

1. Introduction ........................................................................................................................................... 3
2. Commitment ........................................................................................................................................... 4
3. Terms, Concepts and Principles ........................................................................................................... 5
4. Roles, Responsibilities and Reporting .................................................................................................. 15
5. Implementation ..................................................................................................................................... 23

Appendix A: Risk Management Process Overview
Appendix B: Examples of Higher Education Enterprise Risks
Appendix C: Risk Matrix and Heat Map
Appendix D: Enterprise Risk Management Plan
Appendix E: ERM Flow Chart
Appendix F: ERM Implementation Plan Timeline

Document Revision History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Comments</th>
<th>Approved By/Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAFT June 1, 2018 REV 1</td>
<td>Added definition of “Risk Context,” changed “FAeRM” to “FARM,” and added instructions on writing risk identification statements under definition of “Risk Identification.”</td>
<td>Paul Mueller November 20, 2018</td>
</tr>
<tr>
<td>DRAFT June 1, 2018 REV 2</td>
<td>Added Risk Co-Owner, moved assignment of Risk Owners from Division Leadership to Executive Leadership, added Risk Owner support of Executive Leadership at FARM Committee meetings, and replaced Appendix D with an updated version of the Enterprise Risk Management Plan.</td>
<td>Paul Mueller June 10, 2019</td>
</tr>
</tbody>
</table>
1. Introduction

Enterprise Risk Management (ERM) is a structured, institution-wide approach to identifying, assessing, monitoring and responding to enterprise risks within the University’s risk tolerance, to provide reasonable assurance of success in fulfilling the University’s mission and strategic plan. ERM is integrated into the University’s existing governance, decision-making and planning and budgeting processes.

While traditional risk management focuses on institutional loss or damage and minimizing those risks with loss prevention and insurance measures, ERM focuses on risks at an enterprise level. ERM evaluates internal and external factors and influences that may cause uncertainty about whether an institution will achieve its objectives, and seeks to minimize those “risks” with a coordinated management response.

The ERM framework is a set of components that provides resources, terminology, structure and reporting for managing enterprise risks at the University. The framework aligns with International Organization for Standardization ISO 31000 Risk Management Principles and Guidelines.
2. Commitment

The University’s President, Board of Trustees, and Executive Leadership are committed to fostering an environment that will encourage risk-informed decision-making within the University’s culture and practices. The University’s Division Leadership will incorporate ERM into its governance, decision making, and planning and budgeting processes as set out in this framework.
3. Terms, Concepts and Principles

Terms and Concepts

Enterprise Risk Management (ERM)

(See: Appendix A – Risk Management Process Overview)

ERM is a structured, institution-wide approach to identifying, assessing, monitoring and responding to enterprise risks within the University’s risk tolerance, to provide reasonable assurance of success in fulfilling the University’s mission and strategic plan.
Enterprise Risk

(See: Appendix B – Examples of Higher Education Enterprise Risks)

Refers to the effect of uncertainty on the University’s ability to successfully accomplish its mission and strategic plan, including the ability to successfully accomplish division strategic objectives in support of the University’s objectives. Simply stated, they are the things that keep the University from achieving its objectives.

Universities face internal and external factors and influences that make it uncertain whether, when and the extent to which, they will achieve or exceed their objectives. The effect that this uncertainty has on a university’s objectives is enterprise risk.

Opportunity

Taking risks can afford opportunities. The University’s willingness to assume risk will help determine the opportunities it is willing to pursue in order to accomplish its mission and strategic plan. At the operational level, leadership must manage the risk of uncertainty to increase the likelihood of an opportunity’s success.

Risk Context

The risk context is the strategic plan or emerging, strategic initiatives of the University, division or college, or units where ERM is being applied.

Risk Identification

Risk identification is the process of finding, recognizing and describing high-level, enterprise risks (internal and external factors or influences) that may impact the University’s ability to successfully accomplish its mission and strategic plan, or division or unit strategic objectives in support of the University’s objectives. The level of understanding of the risk at this point may be fairly low.

Here are some tips for writing risk identification statements for the matrix:
• Describe the obstacle, challenge, event, harm, financial loss or compliance violation we are trying to address.

• Use plain language, rather than citing a specific compliance rule or regulation, for example.

• Be specific enough for assessment and rating, the next step in the ERM process.

Example: SPACE LIMITATIONS: Inadequate space inventory and/or inefficient use of existing space will negatively impact the University's ability to accommodate its planned growth.

Risk Assessment

Risk assessment is an evaluative process that creates an understanding of the identified enterprise risk to determine where it falls within the University's risk tolerance. It includes an analysis of the risk’s potential impact on the following areas:

• **Strategy:** How the risk may affect high-level goals aligned with and supporting the University’s mission and strategic plan, or division strategic objectives in support of the University’s objectives.

• **Operations:** How the risk may affect the effectiveness and efficiency of the University’s operational and management processes, including performance and accountability goals. Safety is an operational risk.

• **Finances:** How the risk may affect the University’s ability to effectively manage and control the potential loss of financial resources and physical assets.

• **Compliance:** How the risk may affect compliance with relevant external laws and regulations, and internally imposed policies and procedures.

• **Reputation:** How the risk may affect the assets that form the University’s image and reputation with internal and external stakeholders. Although reputation is one of the most important assets of the University, it may not be under the University’s control and only partially mitigated.

Risk assessment also includes a rating of the risks’ potential likelihood and impact on the University’s mission and strategic plan, and prioritization. See Risk Rating and Prioritization.
Risk Rating and Prioritization

(See: Appendix C – Risk Matrix and Heat Map)

Identified enterprise risks are rated using the risk matrix and heat map on a two-dimensional scale considering both the likelihood of the risk occurring and the impact on the University if the risk event should occur, which assists in the prioritization of risks as well. Using a five-point scale, each risk is rated considering the following and then prioritized based on the results:

- **Risk Rating:**

<table>
<thead>
<tr>
<th>Risk Likelihood</th>
<th>Scale</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Certain</td>
<td></td>
<td>Expected to occur in most circumstances (e.g. at least once per year)</td>
</tr>
<tr>
<td>4 Likely</td>
<td></td>
<td>Will probably occur (e.g. at least once per 3 years)</td>
</tr>
<tr>
<td>3 Possible</td>
<td></td>
<td>May occur at some time (e.g. at least once per 5 years)</td>
</tr>
<tr>
<td>2 Unlikely</td>
<td></td>
<td>Could occur at some time (e.g. at least once per 10 years)</td>
</tr>
<tr>
<td>1 Remote</td>
<td></td>
<td>Will only occur in exceptional circumstances (e.g. less than once per 10 years)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Impact</th>
<th>Scale</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Severe</td>
<td></td>
<td>Core mission or strategic plan impaired to the extent that achievement unlikely, operationally disabling, very high reputational impact (nation)</td>
</tr>
<tr>
<td>4 Serious</td>
<td></td>
<td>Operations must shift significantly to adjust to conditions created by consequences of risk-related incident or control failure, seriously degrades the achievement of mission or strategic plan, high reputational impact (region)</td>
</tr>
<tr>
<td>3 Significant</td>
<td></td>
<td>Operational changes are necessary to adjust to conditions created by consequences of risk-related incident or control failure, will degrade the achievement of mission or strategic plan to some degree, moderate reputational impact (local)</td>
</tr>
<tr>
<td>2 Moderate</td>
<td></td>
<td>Consequences of risk-related incident or control failure are tangible, but operations remain largely intact and maintain status quo, may or may not degrade the achievement of mission or strategic plan, low reputational impact (university)</td>
</tr>
<tr>
<td>1 Low</td>
<td></td>
<td>Operations are unaffected, but risk awareness and monitoring is appropriate, little or no reputational impact</td>
</tr>
</tbody>
</table>
**Risk Prioritization:**

Prioritization is based on the likelihood of the risk occurring and the impact on the University if the risk event should occur, and where that falls on the heat map.

![Heat Map Diagram]

- **Very High** – *These are risks that the Board of Trustees and Executive Leadership need to know about.* High-level, enterprise-wide risks whose likelihood and impact will seriously threaten 1) the University’s ability to successfully accomplish its mission and strategic plan, and/or 2) the University’s reputation. These risks will be monitored at the Board of Trustee and Executive Leadership level.
High – High-level, enterprise-wide risks whose likelihood and impact may threaten 1) the University’s ability to successfully accomplish its mission and strategic plan, and/or 2) the University’s reputation. These risks will be monitored at either the Board of Trustee, Executive Leadership and/or Division Leadership level, depending on their scope and nature.

Medium – These risks whose likelihood and impact will or may threaten a division’s functional areas, and its ability to successfully accomplish its strategic objectives. These risks may also include unit-level risks identified by multiple functional areas across a division. These risks are managed without formal monitoring by the Board of Directors or Executive Leadership, thus monitored at the division level.

Low - Risks that have little or no impact on the University’s ability to successfully accomplish its mission and strategic plan. These risks are managed and monitored in the normal course of division business.

Risk Tolerance

Refers to the amount of risk, on a broad level, that the University is willing to take on in pursuit of its mission and strategic plan.

For example, a university may have a low risk tolerance related to threats to the health, safety and well-being of its community, damage or loss to its property, unreasonable potential for financial uncertainty and loss, non-compliance with internal and external compliance mandates, and compromising its reputation. While considering the foregoing, the same university may have a higher risk tolerance as it pursues activities, programs or services related to its mission and strategic plan.

Risk Response

Management’s coordination of human, operational, capital, technological, financial and other resources to ensure the selected action is effectively carried out to manage the enterprise risk within the University’s risk tolerance. Elements of a risk response may be incorporated into strategic planning and budgeting processes.
Risk responses include:

- **Avoidance**: Exiting the activity, program or service that gives rise to the risk.

- **Mitigation**: Strategies and methods used to reduce the risk, including, but not limited to, control and management actions that reduce the risk’s impact on strategic objectives, operations, finances, compliance, and reputation.

- **Acceptance**: No response is taken to affect the risk, other than monitor it.

**Risk Profile**

*(See: Appendix C – Risk Matrix and Heat Map)*

A risk profile includes the spreadsheet summary, or risk matrix and heat map, and corresponding enterprise risk management plans (if applicable), of the high-level, prioritized enterprise risks of the institution or division that could challenge the achievement of the University’s mission and strategic plan, or division strategic objectives in support of the University’s objectives. It is developed through use of the ERM process and assigns Risk Owners (and Co-Owners) and Risk Monitors.

**Enterprise Risk Management Plan**

*(See: Appendix D – Enterprise Risk Management Plan)*

A written management plan may be created for **Very High** and **High** rated strategic risks that require increased attention for management and monitoring purposes.

**SCOT Assessment**

A tool commonly used by University stakeholders in a strategic planning setting that identifies and assesses the Strengths, Challenges, Opportunities and Threats (SCOT) of the institution or a division, college or department. Strengths and Challenges are internal factors while Opportunities and Threats are external.
Principles

Enterprise Risk Management (ISO 31000 amended for the University):

Creates and protects value.

ERM contributes to the demonstrable achievement of objectives and improvement of University performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product and service quality, project management, efficiency in operations, governance, and reputation.

Is an integral part of the University’s processes.

ERM is not a stand-alone activity that is separate from the main activities and processes of the University. ERM is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

Is part of decision making.

ERM helps University decision makers make informed choices, prioritize actions, and distinguish among alternative courses of action.

Explicitly addresses uncertainty.

ERM explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

Is systematic, structured and timely.

A systematic, timely and structured approach to ERM by the University contributes to efficiency and consistent, comparable and reliable results.

Is based on the best available information.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts, and expert judgment.
Is tailored.

ERM is aligned with the University’s existing leadership and management processes.

Takes human and cultural factors into account.

ERM recognizes the capabilities, perceptions and intentions of external and internal influences that can facilitate or hinder achievement of the University’s objectives.

Is transparent, as appropriate, and inclusive.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the University, ensures that ERM remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

Is dynamic, iterative and responsive to change.

ERM continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

Facilitates continual improvement of the organization.

The University should develop and implement strategies to improve its enterprise risk management maturity alongside all other aspects of institutional development.

Enterprise Risk Management (University’s additions):

Is tied to strategy.

Enterprise risks are tied to the University’s mission and strategic plan.

Is part of governance.

ERM is part of, and not separate from, the University’s governance, decision-making and planning and budgeting processes. Leadership that is responsible for achieving strategic
objectives will find that risk is an unavoidable part of the decision-making process and that risk-taking should be informed and intentional.

**Is simple and pragmatic.**

Care should be taken not to overcomplicate the application of the ERM to the point of stifling the decision-making processes within the University. Only consider a manageable number of **Very High** and **High** rated enterprise risks that are tied to strategic objectives.

**Leverages existing processes.**

ERM should leverage existing enterprise risk identification and assessment processes, like Strengths, Challenges, Opportunities and Threats (SCOT) processes, planning and budgeting processes, and similar practices.
4. Roles, Responsibilities and Reporting

(See: Appendix E – ERM Flow Chart)

**Board of Trustees**

The Board of Trustees, as part of its normal governance activities, engages in candid conversations at the strategic level with members of Executive Leadership and the Finance, Audit and Enterprise Risk Management (FARM) Committee to fulfill their shared responsibility of ensuring the University’s enterprise risks are appropriately managed and documented as the University pursues its mission and strategic plan.

**Finance, Audit and Enterprise Risk Management (FARM) Committee of the Board of Trustees**

The FARM Committee assists the full Board in fulfilling its responsibility for oversight of the identification, assessment, monitoring and response to enterprise risks, in fulfillment of the University’s mission and strategic plan. The Committee provides strategic oversight of matters related to the integration of ERM into existing decision-making, strategic planning and budgeting processes. The Committee’s duties do not replace or duplicate established responsibilities and delegations for University leadership and management. ([Source: Board of Trustees Rules of Operation – Appendix B, Board Finance, Audit and ERM Committee Charter](#))

**Executive Leadership**

Executive Leadership includes the President, Provost and Vice Presidents. In consultation with the Board of Trustees and the Board’s FARM Committee, they will:

- **Establish Institutional Tone:**
  - Establish “tone from the top” and commit to implementing ERM at the University.
• **Prioritize Institutional Risks:**
  
  o Prioritize the institution risks within the risk profile, considering recommendations from the Institutional ERM Committee.
  
  o Select and recommend **Very High** or **High** rated enterprise risks for FARM Committee monitoring that are tied to the University’s mission and strategic plan.
  
  o Select **Very High** or **High** rated enterprise risks of special interest to Executive Leadership for their monitoring as well.

• **Assign Risk Ownership:**
  
  o Establish clarity regarding ownership of and responsibility for identified risks and direct Risk Owners (and Co-Owners) to develop and implement response plans and provide progress reports. Division Leadership may also be a Risk Owner.
  
  o Ask Risk Owners (and Co-Owners) to create a written enterprise risk management plan for **Very High** and **High** risks requiring increased attention for management and monitoring purposes, and provide copies as requested to the Institutional ERM Committee.

• **Provide Annual ERM Report:**
  
  o Develop and provide an ERM Report to the FARM Committee, with Institutional ERM Committee assistance, on an annual basis with interim updates at each regular meeting, or as requested.

• **Oversee and Monitor Risks:**
  
  o Oversee and monitor management strategies for enterprise risks within and across their respective areas.
Institutional ERM Committee

The Institutional ERM Committee is provided administrative support by Risk, Compliance and Policy Services (RCPS). The committee will:

- **Manage Framework:**
  - Maintain and monitor the performance of the ERM framework, recommend changes and updates to Executive Leadership, and then make approved revisions for its continued success.
  - Provide tools for Division Leadership use to assist with implementing the ERM framework in their areas, including risk matrix, heat map and related forms.
  - Review training programs for Executive and Division Leadership and Risk Owners (and Co-Owners).
  - Provide consultation and support to Division Leadership as those areas implement the ERM framework. However, the committee does not have substantive responsibility for managing enterprise risks within these areas.
  - Monitor and report on the institution’s ERM effort as a single-source for Executive Leadership on an ongoing basis.

- **Create and Maintain Institution Risk Profile:**
  - Collect and organize division risk profiles for creation and maintenance of the institution risk profile.
  - Prioritize the institution risk profile based on division Very High and High rated risks while considering the University’s mission and strategic plan, and deliver to Executive Leadership for further prioritization and oversight.
  - Reconcile division risk profiles with final institutional risk profile and return to respective Division Leadership, identifying those risks that will be monitored by the FARM Committee, Executive Leadership and/or Division Leadership.
• **Create Annual ERM Report:**
  
  o Develop the annual ERM Report on behalf of Executive Leadership for presentation to the FARM Committee, with interim updates at each regular meeting, or as requested.

Committee membership includes:

• Assistant Attorney General
• Assistant Director, Academic Budgeting and Administration, Provost’s Office
• Associate Vice President for Academic Affairs, Provost’s Office
• Associate Vice President, Business and Financial Affairs *(Co-Chair)*
• Compliance Manager and HIPAA Privacy Officer, Risk, Compliance and Policy Services
• Director, Environmental Health and Safety
• Director, Office of Communications and Marketing
• Director, Office of Internal Audit – *Ex Officio*
• Director, Risk, Compliance and Policy Services *(Co-Chair)*
• Faculty Member, University Planning and Resource Committee Representative
• Research Compliance Officer, Research and Sponsored Programs
• Rules (WAC) Coordinator, Risk, Compliance and Policy Services
• Senior Director and COO, WWU Foundation
• Special Assistant to the Vice President for Enrollment and Student Services
• University Policy Manager & Public Records Officer, Risk, Compliance and Policy Services
• Vice Provost for Information Technology/Chief Information Officer
Division Leadership

Division Leadership includes the Provost and Vice Presidents. Using each area’s existing leadership structures by adding ERM responsibilities to their normal management responsibilities, these leaders will:

- **Integrate ERM:**
  
  - Support the ERM framework.
  
  - Ensure that enterprise risks are identified, assessed, monitored and responded to within their division or areas of responsibility.
  
  - Oversee the integration of ERM into the division or area governance, decision-making, and planning and budgeting processes.
  
  - Engage all Risk Owners (and Co-Owners) in the ERM process that may be directly impacted by it.
  
  - Create a “safe” and open environment for which candid discussions can occur during the ERM process.
  
  - Leverage the division’s existing and related enterprise risk processes, like SCOT Assessments.
  
  - Reinforce “tone from the top.” Promote risk management within the division culture and practices.

- **Create and Maintain Division Risk Profile:**
  
  - Create and maintain a division risk profile and provide copies as requested to the Institutional ERM Committee.
  
  - Ensure identified risks are tied to division strategic objectives, in support of the University’s mission and strategic plan.
Prioritize risks based on the ERM framework’s risk rating methodology.

- **Consider Potential Risk Owners:**
  
  - Risk ownership may be within one division, or shared across division lines for enterprise-wide risks, depending on the scope and nature of the risk. Collaboration between divisions may be necessary.
  
  - As part of their Executive Leadership responsibilities, Division Leadership will assign ownership of and responsibility for identified risks to Risk Owners (and Co-Owners), so it may be helpful to consider potential Risk Owners (and Co-Owners) as division risk profiles are being developed.

**Risk Owners (and Co-Owners)**

Risk Owners may be Division Leadership, and/or those likely reporting to Division Leadership, including Deans, Vice Provosts, Associate and Assistant Vice Presidents and Directors, depending on the scope and nature of the risk. Risk ownership may be shared with Risk Co-Owners, and the functional aspects of risk ownership may be assigned to appropriate faculty or staff, but substantive responsibility for managing the risks rests with the Risk Owners. Risk Owners will:

- **Engage in ERM:**
  
  - Engage in the ERM process where enterprise risks are identified, assessed, responded to and monitored.
  
  - Integrate ERM into the Risk Owner’s governance, decision-making and planning and budgeting processes.
  
  - Engage and support:
    
    - Risk Co-Owners for which they share management of enterprise risks; and
    
    - Appropriate faculty and staff who may be assigned functional aspects of risk ownership.
Promote risk management within the Risk Owner’s area.

- **Manage Enterprise Risks:**

  - Develop and implement risk response plans for identified enterprise risks and provide progress reports to Division Leadership.
  
  - Elevate *Very High* or *High* rated enterprise risks to the attention of Division Leadership.
  
  - Create a written enterprise risk management plan for *Very High* and *High* risks requiring increased attention for management and monitoring purposes, or as requested by Division Leadership.
  
  - Assist Executive Leadership with the annual ERM Report presentation to the FARM Committee, and with interim updates at each regular meeting, or as requested.

- **Manage Other Risks**

  - In addition to enterprise risks, there are other risks that should be identified, assessed, monitored and responded to as part of the Risk Owner’s normal course of responsibility. The ERM framework can be used at the “local” level for such purposes as well. See Appendix A – Risk Management Process Overview.

- **Seek Consultation**

  - Proactively engage University resources in consultation (e.g. Environmental Health and Safety, Public Safety, Risk Management, Compliance Management, Ethics Officer, University Communications, Human Resources, Assistant Attorney General, Internal Audit, Policy and Rules Development, Information Technology, etc.) to assist with the risk management effort. University resources have no substantive responsibility for managing risks within the Risk Owner’s area, but serve as consultants and advisors.
**Internal Audit**

Internal Audit provides an ongoing independent assurance function which evaluates the University’s activities to assist the Board of Trustees, the Board’s Finance, Audit and Enterprise Risk Management Committee, and Executive Leadership in the discharge of their oversight and management responsibilities, which includes the ERM effort.

With safeguards described in the Institute of Internal Auditors (IIA) position paper titled *The Role of Internal Auditing in Enterprise-wide Risk Management*, Internal Audit will support the ERM process by: identifying and evaluating enterprise risks; providing advice regarding management’s responses to those risks (but not make decisions about or implement those responses); and evaluating the ERM process itself from the perspective of Internal Audit.
5. Implementation

(See: Appendix F – ERM Implementation Plan Timeline)

The key elements of implementing the ERM framework include the following:

**Implementation of the Institutional Enterprise Risk Management (ERM) Plan**

- **Training**
  
  - Risk, Compliance and Policy Services (RCPS) will develop an online Canvas training tool and a SharePoint site, and in-person training for executive, division and college leadership.

- **Risk Owners (and Co-Owners) - College and Divisional Unit Risk Profiles and Management Plans**
  
  - Each college and divisional unit will create and maintain a risk profile that summarizes and prioritizes risks that may impact their respective area and division.

- **Division Leadership - Provost and Vice Presidents’ Risk Profiles and Management Plans**
  
  - The Provost and Vice Presidents will compile their respective college and divisional unit risk profiles into division risk profiles that summarize and prioritize risks that may impact their division and University.

- **Institutional ERM Committee**
  
  - The Institutional ERM Committee compiles division risk profiles into a draft institutional risk profile, including appropriate written enterprise risk management plans, and submits to Executive Leadership. The Institutional ERM Committee drafts a preliminary ERM Report.

- **Executive Leadership – Institution Risk Profile and Management Plans**
o The Executive Leadership reviews and prioritizes the institutional risk profile and management plans, assigns Risk Owners (and Co-Owners), approves the ERM Report.

o Written enterprise risk management plans will be created by Risk Owners (and Co-Owners) for Very High and High rated strategic risks that require increased attention for management and monitoring purposes.

- ERM Report
  
o The ERM Report is presented by Executive Leadership to the Board of Trustees Finance, Audit and Enterprise Risk Management (FARM) Committee.

Integration of ERM into Existing Management Processes

This involves the integration of ERM response plans by Division Leadership and Risk Owners (and Co-Owners) into existing governance, decision-making, and planning/budgeting processes, and vice versa.

Application of ERM to Emerging, Strategic Initiatives

This involves the application of ERM by Division Leadership and Risk Owners (and Co-Owners) as part of assessing and implementing new, strategic initiatives, thereby improving their chance for success.

Monitoring

The intent of monitoring is to track the performance of the ERM framework itself and the management of enterprise risks by the institution that have been identified within the ERM process.

- Performance of ERM Framework
  
o The performance of the ERM framework is monitored by the Institutional ERM Committee. The ERM framework will be continuously improved through feedback from University stakeholders in an effort to ensure that the
University’s enterprise risk management approach is helpful, valuable, and effective.

- **ERM Framework Use by Management**

  The use of the ERM framework will be evaluated based on the following:

  o Enterprise risks have been reviewed at least annually by divisions.

  o Actionable response plans have been developed and successfully implemented by Risk Owners (and Co-Owners) for each enterprise risk identified under their ERM processes.

  o Downward movement on the enterprise risk rating scale and heat map based on the ongoing implementation of risk response plans.

  o Documentation of the review of enterprise risks within routine and strategic University management functions.

  o ERM framework training established and made available for University stakeholders.
INTRODUCTION

The risk management process can be applied to high-level, enterprise risks that may impact the University’s ability to successfully accomplish its mission and strategic plan, and other risks that may impact division or unit strategic objectives that support the University’s objectives. The process can be an integral part of an area’s management, embedded in the area’s culture and practices, and tailored and scaled to the area’s activities. The process comprises the activities described below:

PROCESS

Step 1: Establish the Context

Context are the strategic objectives and emerging, strategic initiatives of an area, or those parts of an area where the risk management process is being applied.

Step 2: Risk Identification

Risk identification is the process of finding, recognizing and describing high-level, enterprise risks (internal and external factors or influences) that may impact the University’s ability to successfully accomplish its mission and strategic plan, or division or unit strategic objectives in support of the University’s objectives. The level of understanding of the risk at this point may be fairly low. They can also be viewed as things that create uncertainty about the area’s ability to achieve its strategic objectives or do it effectively.

Step 3: Risk Assessment

Risk assessment is an evaluative activity that creates an understanding of the identified risk to determine where it falls within an area’s risk tolerance (usually aligned with the University’s risk tolerance). It includes an analysis of the risk’s potential impact on strategy, operations, finances, compliance and reputation. It leads to decisions on whether a risk needs a response, and on the most appropriate response strategies and methods.
Step 4: Risk Rating

Risks are rated using a risk matrix and heat map (see Appendix C – Risk Matrix and Heat Map) on a two-dimensional scale considering both the likelihood of the risk occurring and the impact on an area if the risk event should occur, which assists in the prioritization of risks as well.

Step 5: Risk Response

Risk response will be one of the following - avoidance, mitigation or acceptance. Risks that are mitigated are controlled or managed to keep them within an area’s risk tolerance, which will likely necessitate the coordination of human, operational, capital, technological, financial and other resources for accomplishment. Elements of a risk response may be incorporated into strategic planning and budgeting processes.

Ongoing: Monitor and Review

An area’s monitoring and review processes should encompass all aspects of the risk management process for the purposes of ensuring the effectiveness of risk response plans, learning lessons from successes and failures, detecting changes in the original context, and identifying emerging risks.

Ongoing: Communicate and Consult

Communication and consultation with external and internal stakeholders and resources should take place during all stages of the risk management process. To assist in the process, it is helpful to engage internal resources for consultation, such as:

- Environmental Health and Safety
- Public Safety
- Risk Management
- Compliance Management
- Ethics Officer
- University Communications
- Human Resources
- Assistant Attorney General
- Internal Audit
- Policy and Rules Development
- Information Technology
Appendix B: Examples of Higher Education Enterprise Risks

- Enrollment management – growth, retention, and contraction
- Information technology (IT) infrastructure, security and support
- Disaster or emergency response and business continuity
- Preparing and responding to a potential active shooter
- Age and condition of facilities and physical plant infrastructure
- Faculty and staff conflict of interest, misconduct and regulatory non-compliance
- Free speech and expression (allowing controversial speakers or groups on campus, while providing safety and security)
- Tuition affordability and perception of "value" by students, parents and other stakeholders
- Title IX regulatory compliance
- Institutional liability, risk and cost related to mismanagement of third-party contracts
- Student high-risk behaviors and mental health
- Researcher compliance and grant contract administration
- Diversity and inclusion of faculty, staff and students
- Managing the risk of the institution’s increasing entrepreneurial initiatives
- Protection of minors while on campus for youth programs, sport camps and other activities
- Health and safety of faculty, staff and students while working, studying and volunteering abroad
- Employment practices claims and lawsuits relating to wrongful termination, discrimination, retaliation and equal opportunity
- Compliance with privacy protection laws, including FERPA, HIPAA, GDPR, etc.
- Academic freedom for faculty to teach or communicate ideas or facts, however controversial, without institutional retaliation or job loss.
- Donor relations and endowment growth
- Recruitment and retention of faculty and staff
- Media relations, including student publications
- Institutional space limitations – Inventory and utilization
## SPACE LIMITATIONS: Inadequate space inventory and/or inefficient use of existing space will negatively impact the University's ability to accommodate its planned growth.

Current academic space is mostly sufficient to meet current course offerings. However, the University's strategic objective is to increase student enrollment, retention and degrees awarded over the next 8 years. Current inventory and utilization will not accommodate this growth.

**Response:**

**MITIGATE**

Hire a consultant to analyze existing space inventories and utilization, and potential space deficits based on the University's strategic objectives. Develop an institutional space plan and budget based on the consultant's report and begin the necessary steps to address the risk.

**Owner(s):**

Space Administration, FDCB, and FM

**Monitor(s):**

Provost/Vice President for Academic Affairs, Vice President for Business and Financial Affairs

**Likelihood:**

5. Certain

**Impact:**

4. Serious

**Priority:**

Very High
## Enterprise Risk Heat Map

### Impact Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Certain</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4. Likely</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3. Possible</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2. Unlikely</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1. Remote</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

### Number of Risks by Priority

<table>
<thead>
<tr>
<th>Risk Priority</th>
<th>Number of Risks by Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>Medium</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
</tr>
<tr>
<td>Very High</td>
<td>1</td>
</tr>
</tbody>
</table>

### Number of Risks by Priority Graph

- **Y-axis (Number of Risks):** 0 - 2
- **X-axis (Risk Priority):** Low to Very High

The graph illustrates the distribution of risks across different priority levels, with the 'Very High' category showing the highest number of risks.
Appendix D: Enterprise Risk Management Plan

Click or tap to enter a date.

**INSERT TITLE**

**DIVISION(S): INSERT ACRONYM(S)**

---

**IDENTIFICATION**

**Identification of Risk:**

Click here to enter text.

**Risk Statement:**

Click here to enter text.

---

**ASSESSMENT & RATING**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Remote</td>
<td>Low</td>
</tr>
<tr>
<td>2. Unlikely</td>
<td>Moderate</td>
</tr>
<tr>
<td>3. Possible</td>
<td>Significant</td>
</tr>
<tr>
<td>4. Likely</td>
<td>Serious</td>
</tr>
<tr>
<td>5. Certain</td>
<td>Severe</td>
</tr>
</tbody>
</table>

**Brief summary of potential impact on:**

**Strategy:**

Click here to enter text.

**Operations:**

Click here to enter text.

**Finances:**

Click here to enter text.

**Compliance:**

Click here to enter text.

**Reputation:**

Click here to enter text.
RESPONSE

Risk Response: Dropdown List

Risk Response Plan:

Click here to enter text.

<table>
<thead>
<tr>
<th>Action Plan</th>
<th>Owner(s)</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OWNERS & MONITORS

Risk Owner: Click here to enter text.

Risk Co-Owner(s): Click here to enter text.

Risk Monitor(s):

☐ BOT Finance, Audit and ERM Committee ☐ Executive Leadership ☐ Division Leadership
Appendix E - Enterprise Risk Management (ERM) Flow Chart

- Board of Trustees
- Finance, Audit & ERM Committee of the Board
- Executive Leadership
- Institutional ERM Committee
- Division Leadership
- Risk Owners

ERMS Report
Institution Risk Profile
Division Risk Profiles - Source of enterprise risks for Institution Risk Profile
Source of enterprise risks for Division Risk Profiles

Internal Audit
Internal Audit Functional Reporting
Risks identified from internal audit surveys and interviews
## Appendix F: ERM Implementation Plan Timeline

### Objectives

<table>
<thead>
<tr>
<th></th>
<th>Summer 2018</th>
<th>Fall 2018</th>
<th>Winter 2019</th>
<th>Spring 2019</th>
<th>Summer 2019</th>
<th>Fall 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Affairs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit Consultation and Training, <em>only as needed</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provost's Office</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College of Science and Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College of Business and Economics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College of Fine and Performing Arts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College of Humanities and Social Sciences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fairhaven College of Interdisciplinary Studies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSP/Graduate School</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huxley College of the Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Western Libraries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Woodring College of Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business and Financial Affairs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enrollment and Student Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University Relations and Marketing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University Advancement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes
- **BOT Reporting**
  - Summer 2018: BOT Report to BOT FARM Committee
  - Fall 2018: ERM Report to Full Board
- **ERM Reports to Full Board**
  - Summer 2019: ERM Report to Full Board
- **Academic Affairs**
  - Unit Consultation and Training, *only as needed*
- **RCPS Develops Training/SharePoint Site**
- **Training, Division and Institutional Risk Profiles, Integration into Existing Management Processes**
- **Finance, Audit and ERM (FARM) Committee**
- **RCPS Develops Training/SharePoint Site**

### Legends
- Yellow: RCPS Develops Training/SharePoint Site
- Green: Training
- Light Green: Risk Owners - College and Divisional Units Develop Risk Profiles and Management Plans
- Medium Green: Division Leadership - Provost and Vice Presidents’ Develop Risk Profiles and Management Plans
- Dark Green: Institutional ERM Committee - Compiles Divisional Profiles into Draft Institutional Risk Profile
- Purple: Executive Leadership - Reviews and Prioritizes Institution Risk Profile and Management Plans
- Gold: ERM Reports to Board of Trustees