Enterprise Risk Management (ERM) Program Primer

Updated March 5, 2018

Prepared by Al Turgeon
Chief Risk Officer (CRO)

For more information about UVM’s ERM program, visit www.uvm.edu/~erm
Introduction
Before delving into the specifics of UVM’s Enterprise Risk Management (ERM) program, I want to acknowledge the efforts of other UVM risk assurance professionals, the engagement of many UVM staff, faculty, and administrators, and the commitment of UVM’s Board of Trustees and executive leadership, especially President Sullivan. UVM has an efficient and effective ERM program that is based on current higher education best practice and principles outlined in International Standard 31000, yet is tailored to UVM’s institutional culture. I especially want to recognize and thank my colleagues, Mary Dewey, Director Risk Management and Safety, and Erica Heffner, Assistant Director Compliance Services, for their ERM efforts, they deserve praise for collaborating and contributing to advancing ERM here at UVM.

ERM is a valuable tool for conducting a strategic, cross-functional review of the University’s operating environment and competitive position. The process has identified issues that affect our ability to achieve our strategic goals, and operational ones that affect our ability to function efficiently and effectively. UVM’s deliberate focus on both institutional “risks” and “opportunities” is something to be proud of – only a few ERM programs do this in higher education.

UVM’s senior leaders use ERM to complement and inform strategic decision-making, and to inform and assure the Board that senior management is identifying and responding to those uncertainties and exposures that may affect the success of the University’s mission, vision, strategic goals, reputation, competitiveness and planned actions.

What is Enterprise Risk Management?
UVM uses the Institute of Internal Auditors 2009 definition of ERM: Enterprise risk management is a structured, consistent, and continuous process across the whole organization for identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect the achievement of its objectives. ERM is different than traditional risk management, in that it focuses on all types of risk. Traditional risk management focuses on hazard, operational and to a degree legal and compliance risk, see Figure 1 below.

Figure 1: ERM vs. Traditional Risk Management
ERM Program History
UVM began implementing ERM in 2008. The University’s senior administration and Board of Trustees saw the value of adopting ERM as a best practice for taking an institution-wide view of risk and opportunity in order to help UVM achieve its strategic goals.

UVM’s ERM program was developed and based on international risk management standard ISO 31000, and from a review of successful and mature higher education ERM programs. Other inputs came from piloting the risk assessment process in the Division of Finance and Administration, and from feedback obtained in interviews with senior management conducted in the fall of 2010 by external consultants Arthur J. Gallagher, Inc. ERM implementation began in January 2011, and culminated with the University’s first ever Risk-Opportunity Portfolio and Register, and Heat Map in 2013. UVM has updated its Risk-Opportunity Portfolio and Register, and Heat Map every year since.

Purpose & Goals
The purpose of UVM’s ERM program is to enhance the University’s ability to achieve its mission, vision, strategic objectives, and strengthen its competitive position by fostering an institution-wide culture of risk and opportunity awareness, by providing a structured, consistent, and continuous process for the early and proactive identification and reporting of material risks and opportunities to senior management and trustees.

In support of this overall purpose, the specific goals of UVM’s ERM program are as follows:

1. Create a culture of risk awareness where employees understand and consider risk in decision-making.
2. Reduce operational surprises and losses.
3. Increase capacity to identify and seize opportunities.
4. Enhance institutional decision-making.
5. Improve the efficiency and effectiveness of institutional risk management efforts.

Governance
As shown in Figure 2 on page 3, UVM’s ERM program is overseen by the Board of Trustees through its Audit Committee. Ultimate authority rests with the President, advised by the President’s Advisory Committee on ERM (PACERM). The PACERM is co-chaired by the Provost (Assistant Provost & Chief of Staff attends meetings for him) and the Vice President for University Relations and Administration. The Vice Presidents for Enrollment Management; Research; Human Resources, Diversity & Multicultural Affairs, Executive Operations and Finance; Vice Provost for Student Affairs; and the Chief Information Officer serve as voting committee members; and the General Counsel, Chief Internal Auditor, Director of Compliance Services and Chief Risk Officer serve in a consultative role.

Day-to-day management of enterprise or portfolio level risks and opportunities are assigned to Responsible Officials (Deans and Vice Presidents) by the President. Day-to-day management of the ERM program is overseen by the Chief Risk Officer for the institution, advised and assisted by the ERM Advisory Committee (ERMAC), a working group of administrators from both academic and
administrative units. The Director of Risk Management and Safety, and the Chief Risk Officer co-chair the ERMAC.

The Risk Assurance Group (RAG) ensures that there is efficient and effective cross-functional coordination among the ERM and other University offices involved in managing institutional risk. RAG members include: General Counsel, Director of Risk Management and Safety, Director of Compliance Services, Chief Internal Auditor, Associate Chief Information Officer and the Chief Risk Officer.

**Figure 2: UVM ERM Governance Structure**

![ERM Governance Structure Diagram]

Administratively, the CRO reports to the Vice President for University Relations and Administration.

**ERM Annual Areas of Focus**
- Conduct Calendar Year (CY) Annual Risk Assessment
- Facilitate Portfolio Level Risk/Opportunity Response and Reporting
- Conduct Targeted Risk Assessments
- Monitor Emerging Risks & Opportunities
- Conduct limited Education and Outreach efforts
Annual Institution-Wide Risk Assessments

The primary focus of the ERM program is the completion of an annual institution-wide risk assessment using the risk assessment process shown in Figure 3 below, which results in an updated University Risk-Opportunity Portfolio and Register, and Heat Map. The risk assessment process begins in late March or early April and ends in late October of each calendar year (CY).

The risk assessment process is also dynamic in that managers at UVM can, at any time, initiate a risk assessment of an emerging risk and/or opportunity that could result in a change in the Risk-Opportunity Portfolio and Register, and Heat Map.

Figure 3: UVM Annual Risk Assessment Process

Steps in UVM’s Annual Risk-Opportunity Management Process

Updated 01.17.2018

1. Context: CRO, RAG
   Understand organizational objectives and external and internal environment
   CRO memo; initiating risk assessment

2. Identify: Interviewees
   Find, recognize, and describe risks & opport.
   Interview notes
   Write a “risk or opport.”
   Preliminary Risk Inventory (PRI)

3. Analyze: ROs, RAG, ERMAC
   Comprehend and determine nature/level of a risk or opport.
   Determine the risk or opport.’s potential impact and likelihood

4. Evaluate: ROs, CRO, PACERM, President
   Review existing mitigation strategies & determine whether the risk or opport.
   is acceptable, confirm impact & likelihood, prioritize risks
   Final risk-opport. portfolio & heat map
   Get President’s approval

5. Respond: ROs, CRO
   Modify the risk by mitigating, avoiding, transferring, or accepting the risk or pursue opport.
   Develop & implement MRPs for portfolio-level risks & opport.
   Get President’s approval
   November > January

6. Monitor: BOT, President, ROs, CRO, RAG
   Continually check & update status of a risk to ID change from response level required or expected.

7. Report & Communicate: ROs, CRO, RAG
   Inform/engage stakeholders on the current state of risks and their management.
   CRO briefs the Audit and Cmte. of the Whole annually in February
   ROs brief their assigned committees based on published annual schedule/ BOT work plans

Legend: BOT – Board of Trustees, CRO – Chief Risk Officer, ERMAC – Enterprise Risk Management Advisory Committee, MRP – Management Response Plan, PACERM – President’s Advisory Committee on Enterprise Risk Management, PRI – Preliminary Risk Inventory, RAG – Risk Assurance Group (includes the CRO, Dir. Risk Management & Safety, Dir. Compliance Services, Assoc. Chief Information Officer, General Counsel, Information Security Officer, Chief Internal Auditor), RO – Responsible Official
The Portfolio (dark red and darkest green band), shown in Figure 4 below contains the institution’s 15-20 highest-priority risks and opportunities which are routinely reported to the President and Board.

The Register (orange and mid-green band), contains the risks and opportunities that are managed by a Vice President and/or Dean.

The Portfolio and Register is developed and vetted through the University’s ERM governance structure, described in Figure 2 on page 3. The President reviews and approves the University Risk-Opportunity Portfolio and Register, and Heat Map, and assignment of responsible officials (RO) to each risk and opportunity in the Portfolio.

Figure 4: UVM Risk & Opportunity Portfolio and Register Heat Map

ROs must develop, maintain and present a Management Response Plan (MRP) for all their assigned portfolio level risks and opportunities to the President and the Board, in accordance with each Board committee’s annual work plan, at least annually. Also the results of the annual risk
assessment, and all accompanying portfolio level MRPs, are presented by the CRO to the Audit Committee, and the Committee of the Whole in February.

**ERM Framework**

A risk assessment process, is just one of several important components of an effective, standards-based ERM framework, see Figure 5 below. UVM has developed and is using this framework:

**Figure 5: UVM’s ERM Framework**

---

**Education & Outreach Activities**

ERM education and outreach are primarily achieved through the annual interview process, targeted risk assessments, and through promoting the ERM website at [http://www.uvm.edu/~erm/](http://www.uvm.edu/~erm/).

The key educational resource is the “*Guide to Risk Assessment and Response*,” which is used to provide a common standard of assessment at the University, and can be accessed on the ERM website at [http://www.uvm.edu/~erm/RiskAssessmentGuide.pdf](http://www.uvm.edu/~erm/RiskAssessmentGuide.pdf).

The Risk Assurance Group (RAG) members all conduct education and outreach for their specific risk assurance functions. Lastly, the CRO also conducts ERM education on a requested basis.

**ERM Contact Information**

For more information, contact UVM’s Chief Risk Officer, Al Turgeon, by phone at (802) 656-9904, email at aturgeon@uvm.edu, and postal mail address: Room 116, 109 S. Prospect St, The University of Vermont, Burlington, Vermont 05405.