University of Massachusetts System-wide Enterprise Risk Management Program

Administration and Finance Committee
December 13, 2021
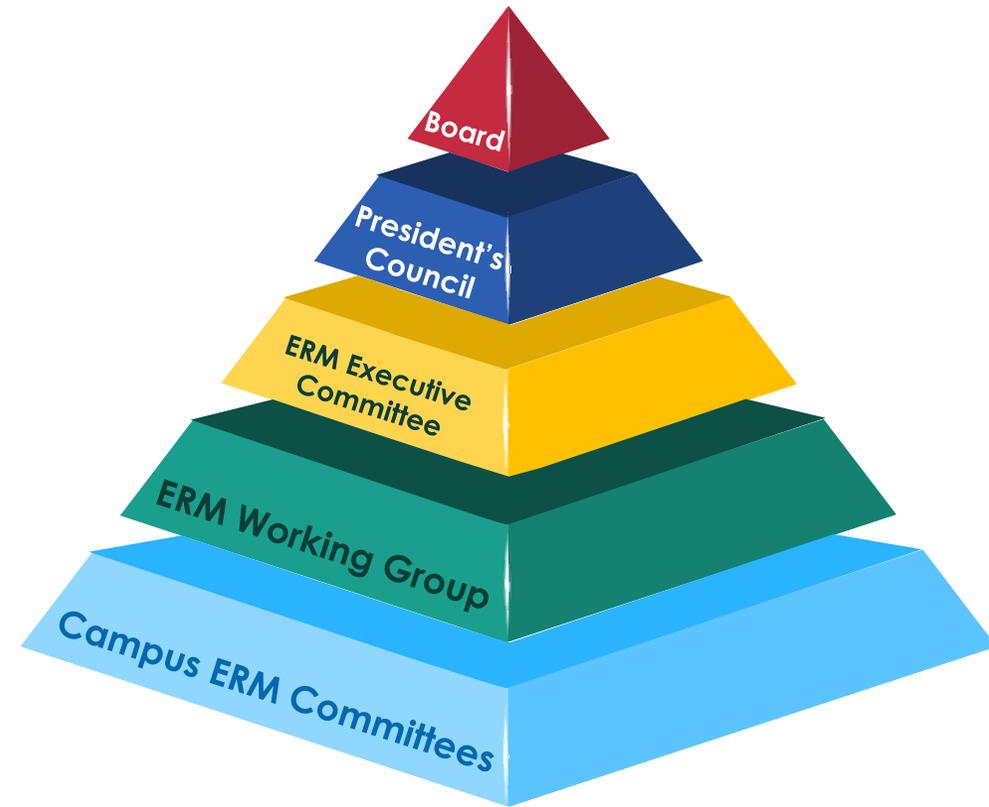
University *of* **Massachusetts**

UMASS

Amherst • Boston • Dartmouth • Lowell • Medical School • UMassOnline

UMass System-wide Enterprise Risk Management Program

- Coordinates system-wide ERM framework through formal governance structure

- Regularly collaborates with:
  - Campus risk and emergency management partners
  - Key partners such as OGC and Internal Audit
  - Additional subject matter experts

- Facilitates process to maintain system-wide Risk Registry
  - Proactively identify, assess & prioritize risks across the University

- Provides transparency and shared understanding of risk across the system at both leadership and operational levels

- Builds capacity and networks to address critical risks, and determines the effectiveness of those strategies

ERM Governance Structure

University *of* Massachusetts

Enhanced ERM Program Cycle

Issue ERM Report · **Identify and Assess Risks** · **Prioritize Risks** · **Identify Risk Mitigation Strategies** · **Assess Risk Mitigation Strategies** · **Implement Risk Mitigation Strategies**

FY21-FY22 Program

- Engaged external expertise and reviewed best practices
  - Conducted comprehensive review of risk assessment tools
    - Expanded evaluation of risk to include legal, compliance and workforce issues
  - Updated risk registry using new risk assessment tools
  - Developing assessment tool for risk mitigation strategies
  - Confirmed alignment with ISO risk management guidelines (31000)

University *of* Massachusetts

UMass ERM Program is at Medium Program Maturity

Progress since FY20: ERM Program moved from mid-range to high range of medium maturity.

- Shifting from reactive to proactive management of risks

- Implementing a regular cycle of identifying, assessing, mitigating and monitoring risks

- Conducting quarterly meetings with the ERM Executive Committee to inform leadership

- Working toward:
  - Increasing visibility of risk mitigation activities
  - Ingraining risk management into everyday culture and activities

Model from AGB; criteria from UE's "Use a Maturity Tool to Advance the ERM Process"

Low-Maturity	Medium-Maturity	High-Maturity
• ERM is reactive to the latest campus crisis or hot topic.	• ERM reacts to past crises while identifying risks to mitigate before they occur.	• ERM identifies emerging risks.
• The ERM process is ad hoc and vulnerable to personalities or bias.	• The ERM process follows the four main steps (identify, assess, plan for/mitigate and monitor risks) and repeats regularly.	• Risks to institutional strategies are considered before adoption.
• The risk management department is responsible for risk treatment.	• Institutional leaders treat ERM as a necessary function to protect the institution.	• The ERM process incorporates the four main steps (identify, assess, plan for/mitigate and monitor risks) and repeats regularly.
• Institutional leaders participate minimally or unenthusiastically.	• Risk management is often undertaken by leaders at the department level, but accountability could be better.	• Risk management is the responsibility of ERM participants who are held accountable for risk treatment.
• Risk treatment focuses on fixing issues.		• Institutional leaders develop a risk-aware culture.
		• ERM manages risks to the institution's mission across silos.

FY20   FY22

University *of* Massachusetts

COVID-19 Tested Our Enterprise Risk Management Program

ERM Program provided a central coordination point/resource for simultaneous response to a significant number of FY20 risks, underscoring the maturity of the program

FY20 Risk Registry			
Risks Impacted by COVID-19			**Risks Not Impacted by COVID-19**
Academic Quality and Standards	Enrollment	Information Security	Building Code Compliance
Alcohol and Substance Abuse	Environmental, Health & Safety Regs	International Activities	Clery Act Compliance
All-hazards Planning	Facilities and Deferred Maintenance	IT Disaster Recovery	Fraud, Waste and Abuse
Attract/Recruit/Retain Faculty/Staff	Financial Sustainability	Labor Relations	Minors on campus
Continuity Planning *	Health Insurance Requirements	NCAA Regulations	Radio Infrastructure*
Crisis Comms Coordination	Immigration Rules	Oversight of Student Organizations	Sexual Assault Policies & Procedures*
Data Management	Immunization Requirements	Student Health & Mental Health Support	Unauthorized Use of Brand
Employment Law/Regulations	Information Privacy	Vendor Management	Uninsured Loss

University *of* Massachusetts

Upcoming ERM Intersections with A&F Roadmap

- Conduct quarterly ERM Executive Committee meetings

- Shift focus of ERM Program to mitigation strategies

- Implement mitigation strategy measurement tool

- Issue FY22 Report in June 2022

University *of* Massachusetts