Enterprise Risk Management

Montana University System

History

The Shift of Risk Management

Definition of Risk

ANYTHING that can harm, prevent, delay, or **enhance** the Montana University System's ability to achieve objectives = RISK

- Risk can be a threat or an opportunity

Transactional Risk Management – Focus on Transferring the Risk

- Insurance
- Specific Hazards
- "Silo" approach
- Risk Manager = Insurance Buyer

Advanced Risk Management – Focus on Reducing Cost-of-Risk

- Alternative risk transfer
- Proactive prevention and risk reduction
- Increased education and accountability
- Risk Manager may be the risk owner

Enterprise-Wide Risk Management – Focus on Optimizing Risk to Achieve Goals

- Broad range of risks
- Alignment with strategic objectives
- Assists in overall resource allocation
- Risks are owned by subject matter experts (SMEs)
- Risk Manager = risk facilitator, partner, leader, but does not own every risk

History

The Shift of Risk Management

Internal Control

1985 – COSO formed in response to unethical business practices of 1970s and 1980s

1992 - COSO's Internal Control Framework

2002 - Sarbanes-Oxley Act

2004 – COSO Releases ERM – Enterprise Risk Management

2006 – SAS 112 – Communicating Internal Control Matters Identified in an Audit

2013 – COSO Internal Control Updated

2014 - Enter the Green Book – Standards for Internal Controls in Federal Government.

- State of Montana policy (MOM 399) requires state agencies develop an Internal Control Framework

2014 – OMB Uniform Grant Guidance

2015 – Fraud Reduction and Data Analytics Act

2016 – OMB A-123 Updated to Require Federal Agencies to implement ERM capability coordinated with strategic planning and review.

Who is interested?

Stakeholders

- Board of Regents
- Budget, Administration, and Audit Committee (BAAC)
- Management
- Risk Management and Tort Division (RMTD) – State
- Legislators
- Community/Public
- Financial Rating Agencies

What Makes ERM Work?

What Makes ERM Work?

General Areas

- Support and Commitment (DC Presentation/Campus Visits)
- BAAC (Training/Discussions)
- Focus on Areas that Add Value (Strategic Objectives)
- Systematic, Structured, and Timely (Framework)
- Risk-Aware Culture / Part of Decision Making (Training/This Takes Time to Build)
- Breakdown of "Silos" / Inclusive / Transparent (Framework/Communications)
- Built in Accountability (Framework)
- Resources (Staff Time/Tools/Training)
- Continual Improvement of Process / Tailored (Framework)

Ownership Model

- BAAC (Sets the tone)
- Executive Risk Committee (Commissioner and Deputy Commissioners)
- University Risk Management Committee (Campus Liaisons)
  - Reporting to senior leaders/executive risk committee/audit committee
- Functional Risk Owners
  - Responsible for implementing risk action plans
  - Assemble work teams
  - Communicate and report
  - Monitor and evaluate
- ERM System
  - Workflow management system

Framework

The Shift of Risk Management

Top Down?

Advantages

- Provides strong governance
- Focus on highest risks
- Ownership assigned to senior level executives
- Backstop for strategic and budgeting plans
- Emerging risk identified/escalated more quickly

Disadvantages

- Disconnect for some employees
- Senior level managers may not know the particulars of risk mitigation efforts
- May show lack of caring what front line staff know and/or positive impacts that they could make

Bottom-Up?

Advantages

- Not another mandate
- Direct involvement and direction from folks that know where skeletons are/what makes the operation tick
- Greater credibility
- More likely to generate candid disclosure/conversations
- Easier to schedule, less formal, more collegiality with accountability.

Disadvantages

- Are we being heard?
- Do they understand or just humoring us?
- Hard to get things done if it’s not a mandate from the Board/Commissioner.

Best Worlds:
Top Down Methodology, supplemented with a Bottom Up Assessment.

Eight ERM Components (COSO)

1. Internal Environment (philosophy, management commitment)
2. Objective Setting (objectives align with mission)
3. Event Identification (risks identified from internal/external events)
4. Risk Assessment (likelihood and impact analyzed)
5. Risk Response (process in place to manage, mitigating strategies to avoid, accept, reduce, transfer, share)
6. Control Activities (policies and procedures to ensure risk response effectively carried out)
7. Information and Communication (relevant, effective, and timely)
8. Monitoring (ongoing management activities and evaluations)

Framework

The Shift of Risk Management

MUS Framework

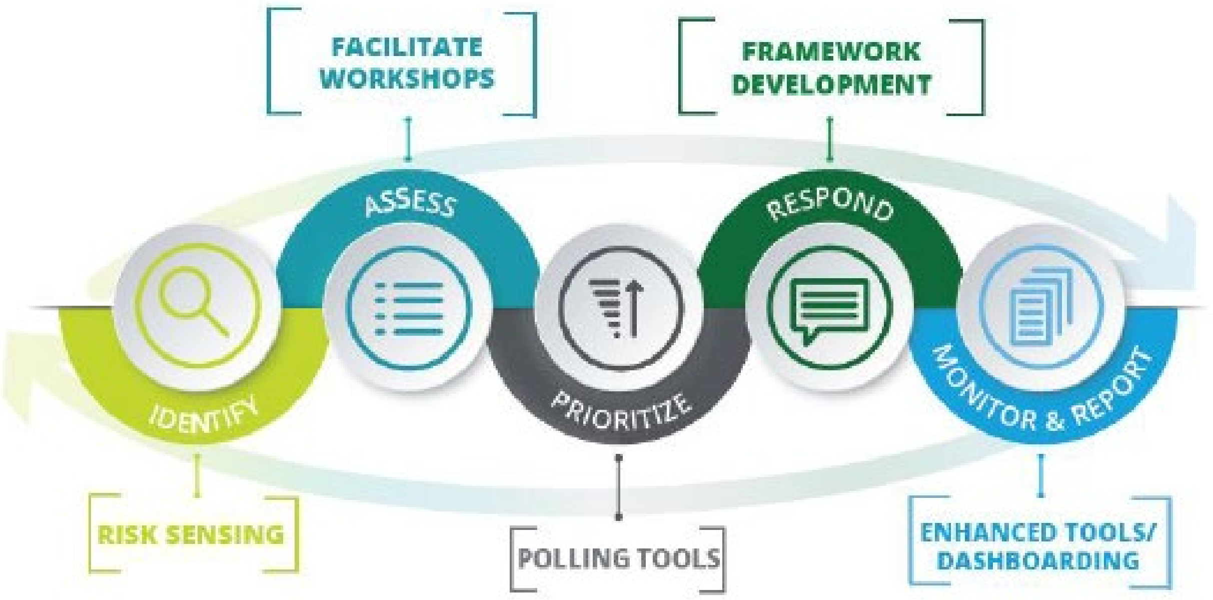
- Keep It Simple/Start Small
- Core ERM Working Group Meeting to Establish Final Assessment Framework and University Risk Management Committee.
  - Identification of Risk Managers Across Campuses

Identify

- Identify and prioritize top 10 risks.
  - Risk Dictionary Developed (Constantly Changing)
    - Over 300+ Risks for Higher Education
  - BAAC Member Risk Areas
  - Commissioner/Deputy Commissioner Workshops
  - Workshops with Presidents/CEOs to establish top 10 risks at each campus and incorporate into core risk list.

Assess/Prioritize

- Core risk list (anticipating 40-60 risks) with MUS Enterprise Risk Committee to add additional details/information for Executive Risk Committee.
- Compile core risk list for Executive Risk Committee to discuss and prioritize system level top 10 risks.



Source: Deloitte/AGB Presentation

Framework

The Shift of Risk Management

Respond – Key in Successful ERM

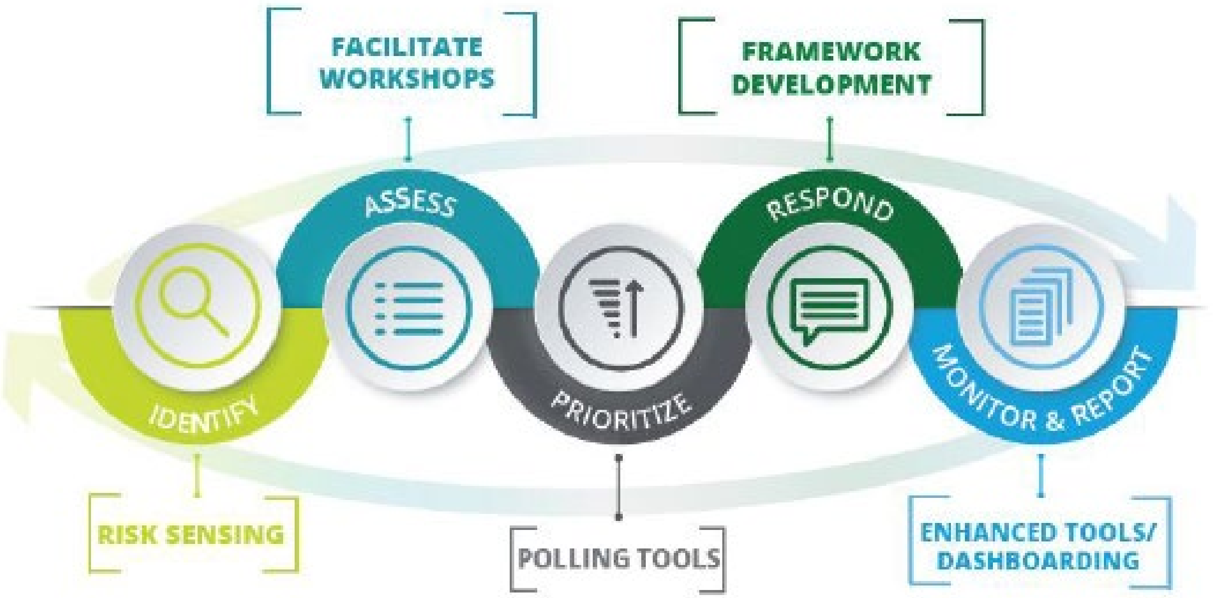
- For areas where further mitigation or action steps need to occur, the Executive Risk Committee will develop:
  - Risk appetite and tolerance levels
  - Risk mitigation plans
  - Assign functional risk owners that are accountable for ensures risk mitigated and aligned with executive committee's risk appetite.

- Process owners may need allocation of funds or resources to bring the risk in alignment with risk appetite and tolerance levels. Strategic budgeting/shared services could potentially assist with this process.

Monitor and Report

- To ensure risks mitigation plans are continually reviewed ongoing monitoring will take place

- In cases where risk needs to be further assessed either Internal Audit from an advisory perspective or other 2nd lines of defense can review.



Source: Deloitte/AGB Presentation

Framework

The Shift of Risk Management

Top Risk Lists – Higher Education

1. Safety and Security
2. Deferred Maintenance
3. Enrollment Management
4. External Environment (political, funding, etc.)
5. Faculty Recruitment and Retention
6. Athletics
7. Behavioral Risk
8. Information Technology
9. Private Partners/Affiliated Organizations
10. Compliance

- Campus safety and security (weather events, violent crime, student & employee health, etc.)
- Information Technology (infrastructure/system security, data security, strategic planning, disaster recovery, etc.)
- Financial resource availability/reliability (state sources, tuition/fees, fundraising, investment return, research grants/contracts, patient revenue, etc.)
- Compliance (state, federal, medical, privacy, research, HR, etc.)
- NCAA compliance (worthy of its own category at Div I institutions)
- Accreditations (institutional, college, school)
- Enrollment management (declining high school grads, scholarship availability, student recruitment/retention, etc.)
- Diversity (students, employees, free speech, inclusivity, etc.)
- Governance (board & senior management)

Global Initiatives (International Programs)
Financial Aid and Scholarships
Admissions and Enrollment
Athletic Travel
Athletic Recruitment
Accounts Payable/Disbursing
Residence Life/Housing
Athletic Title IX
Payroll Services

Financial Management
Information Technology
Research Compliance
Financial Aid
Health and Safety

Bank Reconciliation Process
Contract Management
Fleet Management
International Affairs Review
Student Immunization Review
Athletics Title IX

- ERM process
- System Identity
- Financial Data Integrity
- Financial Forecasting and Stress Testing
- Disaster Planning
- Lab Safety
- Minors on Campus
- Conflicts of Interest
- Cybersecurity
- Institutional Data Integrity
- IT Infrastructure
- Major IT Systems Implementations
- Research Accounting
- Succession Planning – Senior Management and Pivotal Positions

1. Health and Safety of Community (Students, Faculty, Staff, Visitors, etc.)
2. Reputation
3. Decentralized Operations
4. IT/IS Security
5. Financial Planning/Management
6. Intercollegiate Athletics
7. Facilities, Maintenance and Capital Projects
8. Emergency Preparedness

Discussion/Questions

- What are the top risks/concerns committee members have as it relates to the University System?
- What is the committee's expectations of ERM and Internal Audit?
- Anything else committee members would like to discuss as it relates to ERM or Internal Audit?