ERM: A Project Plan for Implementation

April 13, 2016

Tim Wiseman
Assistant Vice Chancellor for Enterprise Risk Management and Military Affairs
East Carolina University
Learning Objectives

At the end of this session, you will have:

• identified key steps involved in planning and implementing an effective enterprise risk management (ERM) program
• heard strategy considerations to meet ERM program goals
• been introduced to the ISO 31000 risk management framework and its relationship to ERM planning and program establishment
• reviewed tools to use in building the foundation of an ERM implementation plan
• gained insight into one organization’s approach to ERM implementation
Agenda

- Frames of Reference
- Mission Analysis and Determination of Key Tasks
- Mission Essential Task List
- Lines of Operations
- After Action Reviews - Sustainment of the Enterprise Risk Management Effort
- Questions / Discussion
Agenda

- Frames of Reference
- Mission Analysis and Determination of Key Tasks
- Mission Essential Task List
- Lines of Operations
- After Action Reviews - Sustainment of the Enterprise Risk Management Effort
- Questions / Discussion
THEN AND NOW
YIKES!
East Carolina University

Location
Military Concepts and Terms

• **Mission**
  – Mission Analysis
  – Specified and Implied Tasks
  – Task, Conditions, and Standard

• **Enemy**

• **Friendly Forces and Allies**

• **Mission Essential Task List (METL)**
  – Battle Tasks

• **Lines of Operation (LOO’s)**

• **After-Action Reviews**
Agenda

• Frames of Reference
• Mission Analysis and Determination of Key Tasks
• Mission Essential Task List
• Lines of Operations
• After Action Reviews - Sustainment of the Enterprise Risk Management Effort
• Questions / Discussion
Mission Analysis

1. Analyze the higher headquarters' order.
2. Conduct initial intelligence preparation of the battlefield (IPB).
3. Determine specified, implied, and essential tasks.
4. Review available assets.
5. Determine constraints.
6. Identify critical facts and assumptions.
7. Conduct risk assessment.
8. Determine initial commander's critical information requirements (CCIR).
9. Determine the initial reconnaissance annex.
11. Write the restated mission.
12. Conduct a mission analysis briefing.
13. Approve the restated mission.
14. Develop the initial commander's intent.
15. Issue the commander's guidance.
16. Issue a warning order.
17. Review facts and assumptions.
ECU’s ERM Environment

- Public versus private institution
- Heritage and traditions
- Demographics and location/proximity
- Part of a system versus independent
- Research, medical campus, vision/objectives, interface with society & community
- Size and scale
- Budget and capital projects
- “Nonprofit”
- Shared governance
- Academic core
- Increased regulation and federal/state oversight

Main University Risk Categories:

- Strategic
- Financial
- Operational
- Compliance
- Reputational -> Overarching
Enemy

- Obsolescence
- Irrelevance
- Loss of “market share”
- Loss of stakeholder trust and/or perceived value
- Avoidable or unnecessary uncertainty
- Underperformance or consistently failing to meet performance and strategic objectives
- Catastrophic loss (real and/or reputational) beyond institution’s capability to recover in the short term and forces a surrender of one or more strategic objectives
Friendly Forces & Allies

- Internal Audit
- General Counsel – Office of the University Attorney
- Internal Control Program
- Environmental Health and Campus Safety
- University Safety and Concerns Committee
- Identity Theft Prevention Committee
- Compliance Offices
- Board of Trustee Expertise
- Task Forces or Working Groups
- Other Pre-existing Entities

*Integrate, Integrate, Integrate and take advantage of bi-products and spin-offs from other initiatives!*
Tone at the Top

• Board of Trustees Audit Committee

• “Chancellor’s View” Fall/Winter 2009:

  ➢ Our goal at East Carolina University is to have the best possible systems for controlling our risks and for internal auditing.

Enterprise risk management is a holistic, comprehensive approach to risk identification and prioritization ultimately leading to better governance, strategic decision making, resource allocation and stewardship.
A mature ERM program is proactive and prevention oriented. It does not replace or interfere with our necessary internal auditing functions, but rather is complementary and reinforcing.

The enterprise approach strives to develop a mindset that makes people at multiple levels ask: "Who else needs to know?" and "Whom haven’t I told?"

Enterprise risk management is a strategic enabler for ECU Tomorrow.

Done right, ERM will allow us to be good stewards of our resources and may reduce reportable audit findings as we self-identify areas of concern and mitigate the risks before vulnerability is exploited.
Break large tasks down into smaller bites:

...... what task is to be accomplished?,

...... under what condition (or range of conditions)?, and

...... to what measurable standard?
Sources of Information

- ANSI/ASSE/ISO 31000 – the *only* international standard on risk management – 2009
- COSO ERM Framework – 2004
- Consulting firms – KPMG, Protiviti, Deloitte, PwC & brokerage firms, too
- GRC – Governance, Risk & Compliance (software and consulting)
ROAD TO IMPLEMENTATION
Enterprise Risk Management for Colleges and Universities

Gallagher Higher Education Practice

www.ajg.com

(Collaborative Risk Management:
“Risk Management” vs. “Managing Risk”)

(Download these at no charge)
ANSI/ASSE/ISO Risk Management Standards Package

Principles

- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available info
- Tailored
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive to change
- Facilitates continual improvement & enhancement of the organization

Framework

- Mandate & Commitment
- Design framework for managing risk
- Implement risk management
- Continually improve the framework
- Monitor and review the framework

RM Process

- Establish the context
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitor and review
- Communicate and consult

From ANSI/ASSE/ISO 31000
Principles

• Creates value
• Integral part of organizational processes
• Part of decision making
• Explicitly addresses uncertainty
• Systematic, structured & timely
• Based on best available info
• Tailored
• Takes human & cultural factors into account
• Transparent & inclusive
• Dynamic, iterative & responsive to change
• Facilitates continual improvement & enhancement of the organization

The principles provide guidance on the rationale for managing risk and the characteristics of effective risk management

These shape the design and structure of your framework for managing risk

The principles can assist in continual improvement and serve as a “maturity model” for implementation
Based upon a model of continual improvement, the framework is what will sustain your risk management efforts. This assures that you are consistent, process-focused and held accountable.

Building the framework includes planning for implementation, monitoring & review and communication.
• The *context* applies to both the organization as a whole and the specific project, risk or portfolio of risks

• Several elements take stakeholder interest and *perceptions* into account

• Monitor and review – continually asks: “Do we have this right?”

• Communication and consultation is how the management of risk stays *connected* and *relevant*

• The same consistent process used across the organization
Specified and Implied Tasks

What have “you” been specifically told to accomplish? (specified)

What other related actions do you think may have been assumed, overlooked, or implied as a part of specific directives for your risk management program? (implied)

*It is important to wrap your arms around both specified and implied tasks to ensure you can fully meet the objective.*
Our Mission:  Provide leadership and management experience to better identify and manage the university’s strategic, financial, operational, regulatory compliance, and reputational risks holistically as an enterprise.

ECU’s ERM Approach:

• Work through the Enterprise Risk Management Committee in a decentralized fashion to accomplish ERM goals
• Improve risk measurement to support strategic decision making, risk mitigation efforts, and resource allocation
• Use pre-existing risk identification and internal control processes to the greatest extent possible
• Raise institutional awareness of existing and emerging risks and their relative potential effects on the institution as a whole
• Provide training and relevant information on ERM to enhance the internal controls and risk management mindset of ECU employees, students, and other stakeholders
Agenda

• Frames of Reference
• Mission Analysis and Determination of Key Tasks
• Mission Essential Task List
• Lines of Operations
• After Action Reviews - Sustainment of the Enterprise Risk Management Effort
• Questions / Discussion
“Do essential things first. There is not enough time for the commander to do everything. Each commander will have to determine wisely what is essential, and assign responsibilities for accomplishment. He should spend the remaining time on near essentials. This is especially true of training. Nonessentials should not take up time required for essentials.” General Bruce C. Clarke

Battle Tasks: Supporting tasks that are necessary to achieve their related mission essential task.
ERM Road Map

Phase 1: Building the Case for ERM
1. Understand the institution’s plans, environment, and culture
2. Determine the status of your existing risk management processes
3. State your goals and objectives
4. Present the case
5. Obtain top-level commitment, support, and participation

Phase 2: Building an ERM Foundation
6. Name a project leader
7. Plan your project and incorporate a timeline
8. Select or design an ERM Framework that best fits the institution’s goals and campus culture
9. Create a cross-functional Risk Council
10. Create a mission and goals statement for the Risk Council
11. Develop a risk vocabulary and definitions

Phase 3: Implementation
12. Develop a risk portfolio
13. Assess your risks: validate and prioritize
14. Assign ownership and take action

Phase 4: Sustaining Your ERM Program
15. Assess results
16. Review and realign risk treatments with available resources
17. Meet and Report
18. Do not neglect traditional risk management functions
19. Review any ERM framework you have followed
20. Develop institution-wide systems for communicating (ongoing)

Estimated progress point to date – 56 months (2013)

Road to Implementation, Enterprise Risk Management for Colleges and Universities, Gallagher Higher Education Practice, 2009
<table>
<thead>
<tr>
<th></th>
<th>Risk Description/Title</th>
<th>Major Risk Category</th>
<th>Previous Top Ten List?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Facilities Obsolescence and Deferred Maintenance</td>
<td>Operational</td>
<td>NO</td>
</tr>
<tr>
<td>2.</td>
<td>Additional State Budget Cuts</td>
<td>Financial</td>
<td>YES</td>
</tr>
<tr>
<td>3.</td>
<td>No or Insufficient Salary Raises Over Multiple Years and Corresponding Effect on Faculty-Employee Morale</td>
<td>Financial</td>
<td>NO</td>
</tr>
<tr>
<td>4.</td>
<td>Potential For Losing a Significant Number of Subject Matter Experts and Senior Administrators Due to Retirement Eligibility – Succession Planning (Continuity)</td>
<td>Operational</td>
<td>YES</td>
</tr>
<tr>
<td>6.</td>
<td>Data and Information Security – Vulnerability to Cyber Attacks and Potential Loss or Compromise of Sensitive Data/Information</td>
<td>Operational</td>
<td>YES</td>
</tr>
<tr>
<td>7.</td>
<td>Increasing Federal Requirements and Compliance Expectations During a Time of Significant Budget Cuts</td>
<td>Compliance</td>
<td>YES</td>
</tr>
<tr>
<td>8.</td>
<td>Continued Decline in Graduate Program Enrollment</td>
<td>Operational</td>
<td>NO</td>
</tr>
<tr>
<td>9.</td>
<td>Reputational Risk Associated with Media-Accelerated/Induced Negativity Related to Non-Compliance</td>
<td>Compliance / Reputational</td>
<td>NO</td>
</tr>
<tr>
<td>10.</td>
<td>Personnel Strain Related to Oversight and Management of Ever-Growing Spread of Projects, Activities, and Opportunities</td>
<td>Operational</td>
<td>YES</td>
</tr>
</tbody>
</table>
# Private Sector Top Risks

<table>
<thead>
<tr>
<th>Private Sector CEO Survey Risk Description/Title</th>
<th>Appears on ECU Top Ten List?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Regulatory Change and Heightened Regulatory Scrutiny</td>
<td>YES</td>
</tr>
<tr>
<td>2. Economic Conditions</td>
<td>YES</td>
</tr>
<tr>
<td>3. Cyberthreats</td>
<td>YES</td>
</tr>
<tr>
<td>4. Succession Challenges and Ability to Attract and Retain Top Talent</td>
<td>YES</td>
</tr>
<tr>
<td>5. Organization's Culture</td>
<td>NO</td>
</tr>
<tr>
<td>6. Organizational Resistance to Change</td>
<td>NO</td>
</tr>
<tr>
<td>7. Privacy/Identity Management and Information Security</td>
<td>YES</td>
</tr>
<tr>
<td>8. Crisis Management</td>
<td>NO</td>
</tr>
<tr>
<td>9. Sustaining Customer Loyalty and Retention</td>
<td>YES (Enrollment)</td>
</tr>
<tr>
<td>10. Meeting Performance Expectations</td>
<td>NO</td>
</tr>
</tbody>
</table>

(Source: NC State ERM Initiative/Protiviti, 3rd Annual Survey of Board Members and C-Level Executives, www.protiviti.com/toprisks)
Agenda

- Frames of Reference
- Mission Analysis and Determination of Key Tasks
- Mission Essential Task List
- Lines of Operations
- After Action Reviews - Sustainment of the Enterprise Risk Management Effort
- Questions / Discussion
## Lines of Operations

<table>
<thead>
<tr>
<th>LOOs</th>
<th>Supporting Tasks</th>
<th>End State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform and Educate About ERM Principles</td>
<td></td>
<td>Risk Intelligent Organization</td>
</tr>
<tr>
<td>Support ERM Committee</td>
<td></td>
<td>Active Committee Assisting with Risk Advice / Sensing/ Mitigation &amp; Treatment</td>
</tr>
<tr>
<td>Provide Risk Consultation Services</td>
<td></td>
<td>Risk-Informed Decision Making</td>
</tr>
<tr>
<td>Conduct Risk Research and “Library” Services</td>
<td></td>
<td>Readily Available Info-Pathways for “Constituents”</td>
</tr>
<tr>
<td>Mature and Sustain the ERM Program</td>
<td></td>
<td>ERM Processes Fully Adopted/Embedded in Culture</td>
</tr>
</tbody>
</table>
# ERM Activities Model

## Two-Year Approach

<table>
<thead>
<tr>
<th>Year</th>
<th>Primary Activities</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Even “On” Year</td>
<td>• Full ERM Risk Survey</td>
<td>• Engaging Key Sensors</td>
</tr>
<tr>
<td>(example: ’14-’15)</td>
<td>• Full Risk Prioritization Exercise</td>
<td>• Assessment Process (Rigor and Detail)</td>
</tr>
<tr>
<td></td>
<td>• Reset</td>
<td>• Risk Register Update</td>
</tr>
<tr>
<td></td>
<td>• Board of Trustees and Exec-Level Presentations and Involvement</td>
<td>• Fresh Look at Current and Anticipated Risk Environment</td>
</tr>
<tr>
<td></td>
<td>• Risk Management Plans Creation (or Updates)</td>
<td></td>
</tr>
<tr>
<td>Odd “Off” Year</td>
<td>• Smaller Scale Re-Prioritization/Re-Validation Exercise</td>
<td>• Risk Management Plans Update/Adjustment</td>
</tr>
<tr>
<td>(example: ‘13-’14)</td>
<td>• Departmental Workshops</td>
<td>• “By Exception” Reviews</td>
</tr>
<tr>
<td></td>
<td>• Interviews and Sensing Sessions</td>
<td>• Select Risk Management Project Work</td>
</tr>
<tr>
<td></td>
<td>• Presentations to Other Key Committees/Groups</td>
<td>• ERM “Maturity” Assessment(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Education</td>
</tr>
</tbody>
</table>
EVERYONE IN THE MILITARY DOES THEIR JOB.

AND THEN THERE'S STEVE...
Agenda

- Frames of Reference
- Mission Analysis and Determination of Key Tasks
- Mission Essential Task List
- Lines of Operations
- After Action Reviews - Sustainment of the Enterprise Risk Management Effort
- Questions / Discussion
An after action review (AAR) is a structured review or de-brief process for analyzing what happened, why it happened, and how it can be done better by the participants and those responsible for the project or event.
# ERM Milestones

<table>
<thead>
<tr>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CRO Hired</td>
<td>• 1&lt;sup&gt;st&lt;/sup&gt; ERM Survey</td>
<td>• Hosted NC ERM in Higher Ed Symposium</td>
<td>• Migrated ERM Survey to Qualtrics</td>
<td>• Risk Working Groups</td>
<td>• Risk Assessment Tool Development</td>
</tr>
<tr>
<td>• Risk Committee Established</td>
<td>• Board Audit Committee Inclusion</td>
<td>• Standardized ERM Briefing Formats</td>
<td>• ERM Workshop on Health Sciences Campus</td>
<td>• Risk Mgmt Process Owners</td>
<td>• 2-Year ERM Cycle Model Adopted</td>
</tr>
<tr>
<td>• Senior Leader Expectations Published</td>
<td>• Implementation Road Map and Strategy Introduced</td>
<td>• Risk Identification Workshop for Academic Deans and Directors</td>
<td>• Office Calls with Executive Council Members</td>
<td>• ERM Training Sessions – Webinar Series</td>
<td>• Enhanced ERM Materials “Push” to Full Board</td>
</tr>
<tr>
<td>• ERM Training (TXAMU Visit)</td>
<td>• SharePoint Site Established</td>
<td>• ERM Involvement on Crisis Policy Team</td>
<td>• Introduced Risk Reviews Format</td>
<td>• Robust Risk Presentation to Executive Council and Board Audit Committee</td>
<td>• ERM Form Development</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Risk Survey Results Briefed to Leadership</td>
<td></td>
<td>• Connection with College of Business Risk Management Faculty/ Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ERM on Key Committees</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ERM Successes

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Risk Committee</td>
<td>• Interview/Survey Balance</td>
</tr>
<tr>
<td>• Relationship with Counsel and IA</td>
<td>• Board and Senior Leader Support</td>
</tr>
<tr>
<td>• Collaboration and Partnership</td>
<td>• SharePoint Reference Library</td>
</tr>
<tr>
<td>• ERM Orientation Packets</td>
<td>• Consultation “Niche”</td>
</tr>
<tr>
<td>• Weekly and Quarterly Reports</td>
<td>• Early Wins (Mgmt Corrective Actions, Deposits Transport, Etc.)</td>
</tr>
<tr>
<td>• Establishing an ERM “Rhythm”</td>
<td>• Increasing Inclusion in Consultations and Evaluation Actions</td>
</tr>
</tbody>
</table>
## ERM Challenges

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Acceptance of the ERM (and Risk Officer) Role and Function</td>
<td>• Measuring and Demonstrating Tangible Value</td>
</tr>
<tr>
<td>• Allocating Time to Training vs Recordkeeping vs Promoting / Marketing vs Analysis</td>
<td>• Mid-Level Management Buy-In</td>
</tr>
<tr>
<td>• Departmental Adoption of ERM Principles and Practices</td>
<td>• Continuous “Re-Introduction”</td>
</tr>
<tr>
<td>• Maintaining Distance but not Being Aloof</td>
<td>• Establishing and Maintaining Trust – Combating Departmental Defensiveness</td>
</tr>
<tr>
<td>• Merging ERM with Ongoing Initiatives</td>
<td>• Getting ERM Included Early Enough in Decision-Making and Strategic Planning</td>
</tr>
</tbody>
</table>
Road Ahead

ERM Program Trajectory Options

Resource Level

Best Practice Champion/Thought Leader and Practitioner – Fully Enabled C-Suite Status with Staff and Dedicated IT RMIS Platform. Influence Extends Beyond ECU’s Boundaries.

Consolidated Risk Mgmt “Center of Excellence” - Under One Roof

ERM Integrator – Multiple Organizational Levels (Workshops, Tools, Analysis, Visibility-Enhanced)

Strategic Planning and Decision-Making Integration/ERM Best Practice Champion


Outcomes vs. Resources
Road Ahead

Notional Risk Management and Compliance Center - Institutional Level

Chief Risk and Compliance Officer (VC-ERM&C or DRM&C)

Admin Associate/Exec Asst

Risk Management - Insurance

Insurance Assistant

Insurance Assistant

Workers Compensation

Enterprise Risk Management Analyst/Project Mgr

Compliance Assistant/Analyst

Divisional Compliance Officers (Athletics, R&GS, ITCS, HSC, Other?)
We try to eliminate some hits and avoid or reduce the clobbers....
Agenda

• Frames of Reference
• Mission Analysis and Determination of Key Tasks
• Mission Essential Task List
• Lines of Operations
• After Action Reviews - Sustainment of the Enterprise Risk Management Effort
• Questions / Discussion
Questions / Discussion?