PRIMA'S 2016 RISK MANAGEMENT
WEBINAR SERIES

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.
10. Plan use of available time.
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.

Tone at the Top (Continued)

- 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.

Task, Condition, Standard

Break large tasks down into smaller bites:

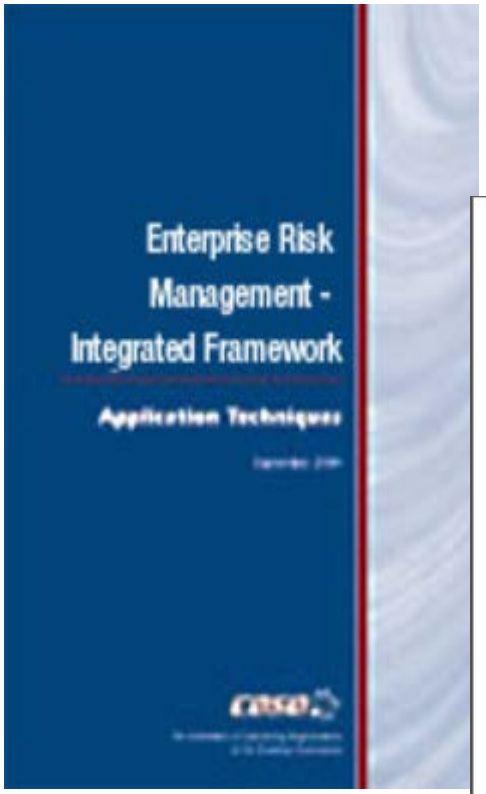
…… what task is to be accomplished?,

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

…... to what measurable standard?

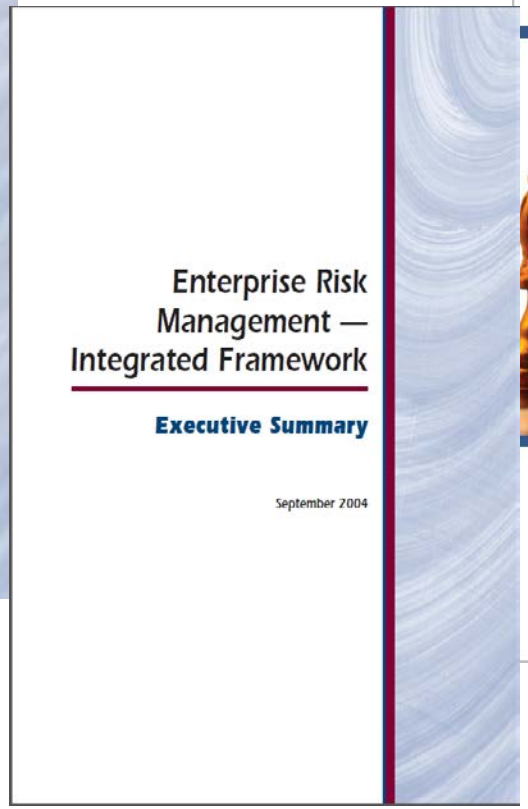
Sources of Information

- ANSI/ASSE/ISO 31000 – the *only* international standard on risk management – 2009
- COSO ERM Framework – 2004
- “Risk Management – An Accountability Guide for University and College Boards” by Janice Abraham – AGB & UE – 2013
- Consulting firms – KPMG, Protiviti, Deloitte, PwC & brokerage firms, too
- GRC – Governance, Risk & Compliance (software and consulting)

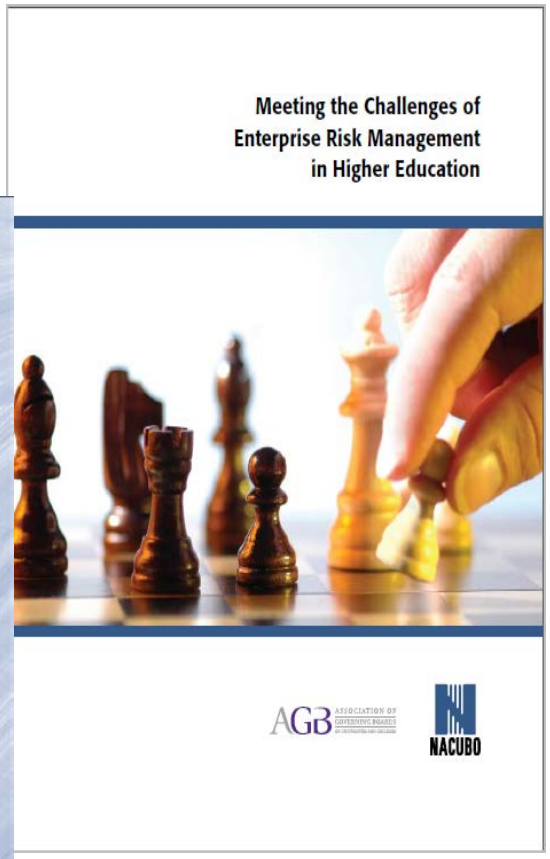


www.coso.org

$$

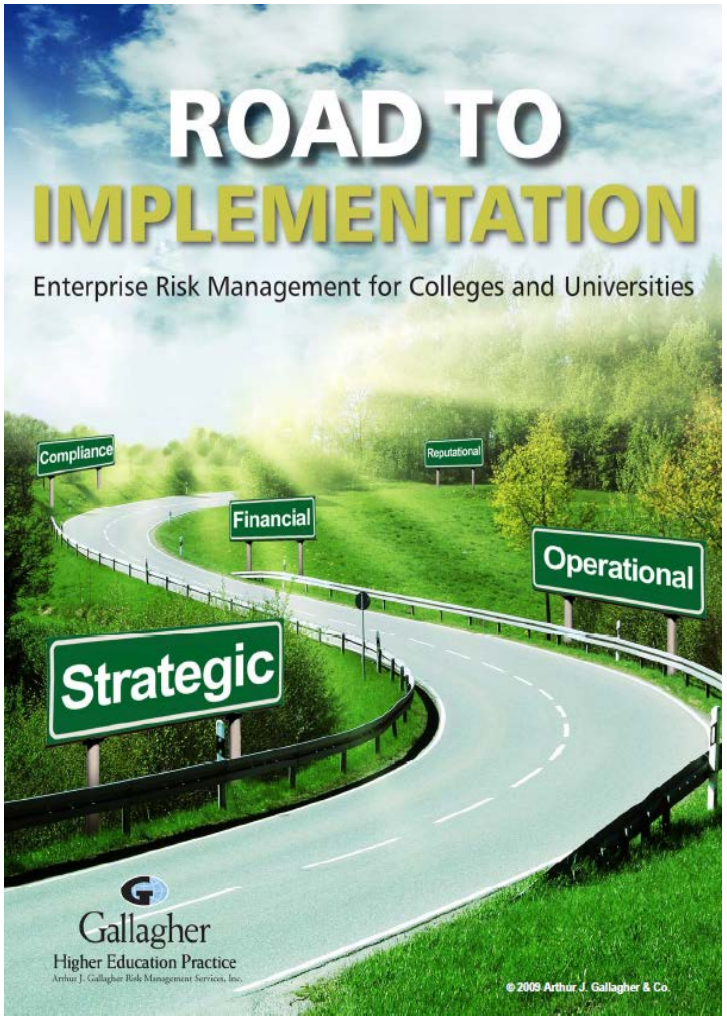


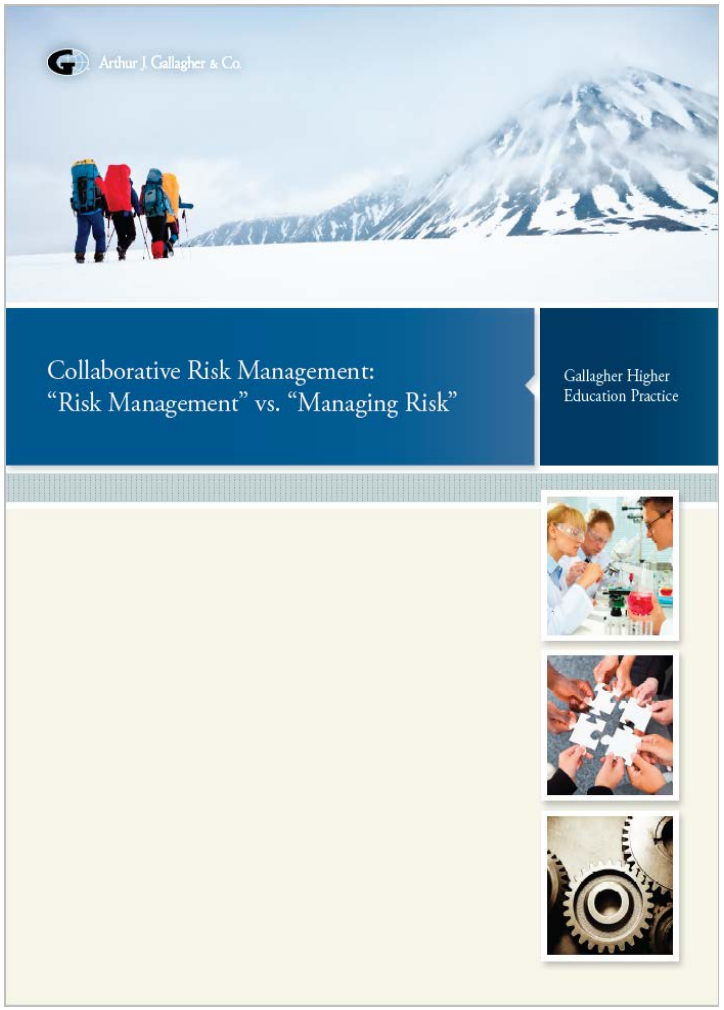
(Download this one free)



www.nacubo.org

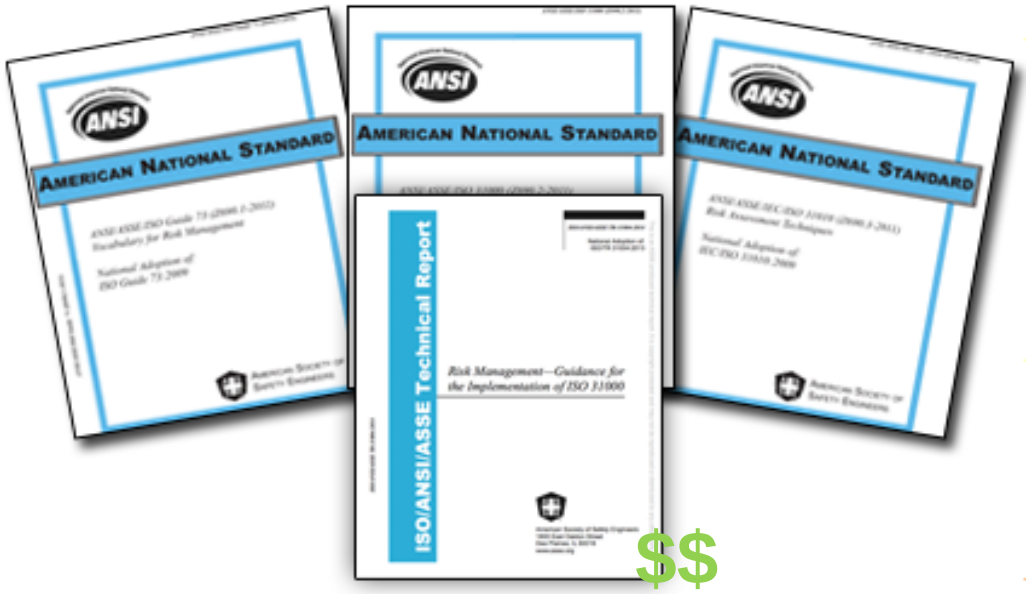
(Download this one free)





www.ajg.com

(Download these at no charge)



www.asse.org

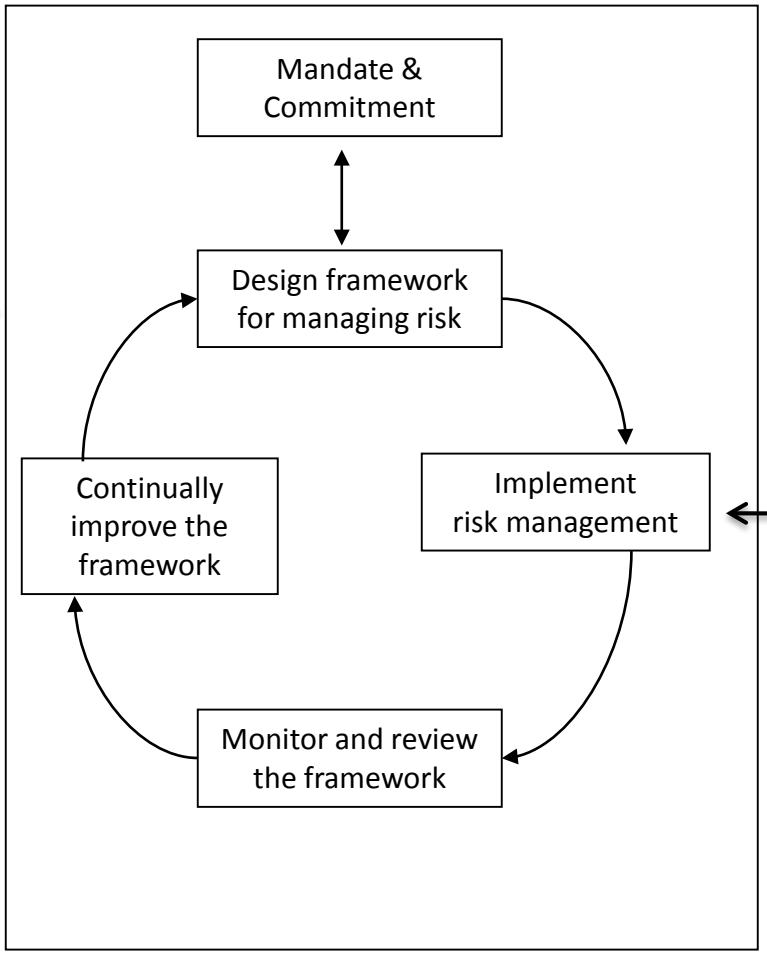
ANSI/ASSE/ISO Risk Management Standards Package

ISO/ANSI/ASSE/TR-31004-2014 (Z690 TR-2014) Risk Management-Guidance for the Implementation of ISO 31004
(identical national adoption of ISO/TR 31004:2013)
ANSI/ASSE/ISO Guide 73 (Z690.1-2011) Vocabulary for Risk Management
(identical national adoption of ISO Guide 73:2009)
ANSI/ASSE/ISO 31000 (Z690.2-2011) Risk Management—Principles and Guidelines
(identical national adoption of ISO 31000:2009)
ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011) Risk Assessment Techniques
(identical national adoption of ISO/IEC 31010:2009)

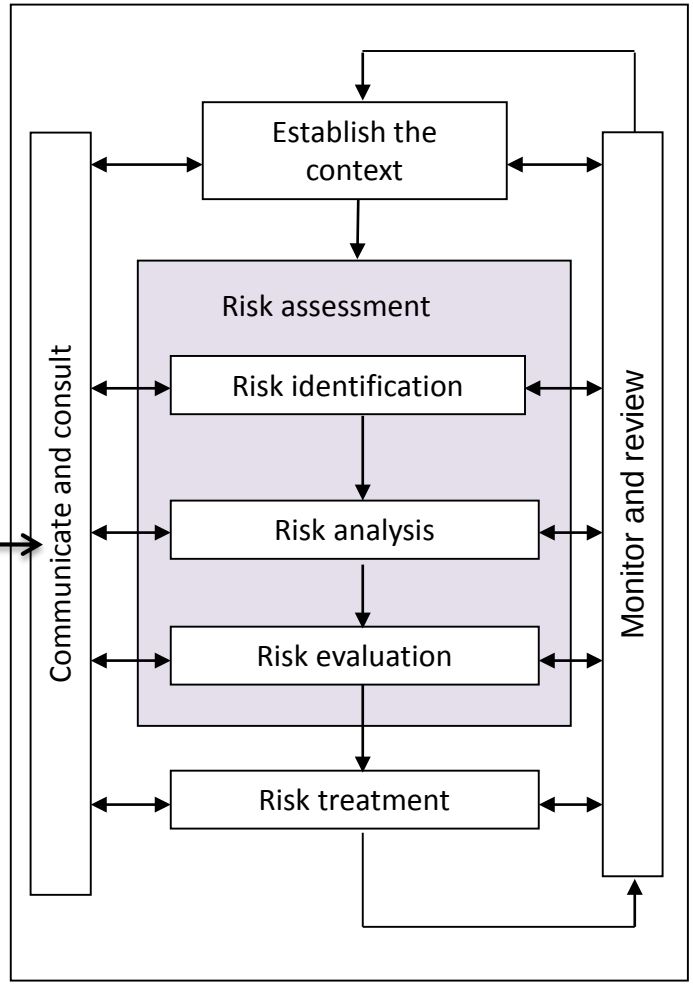
Principles

- 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



RM Process



From ANSI/ASSE/ISO 31000

Principles

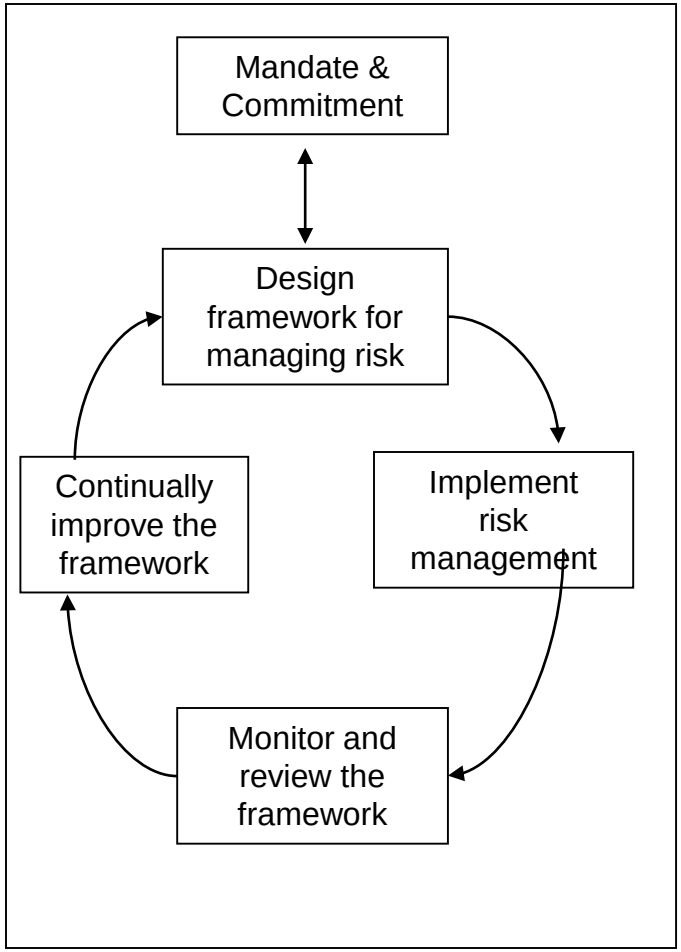
- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available info
- Tailored
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive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

Framework



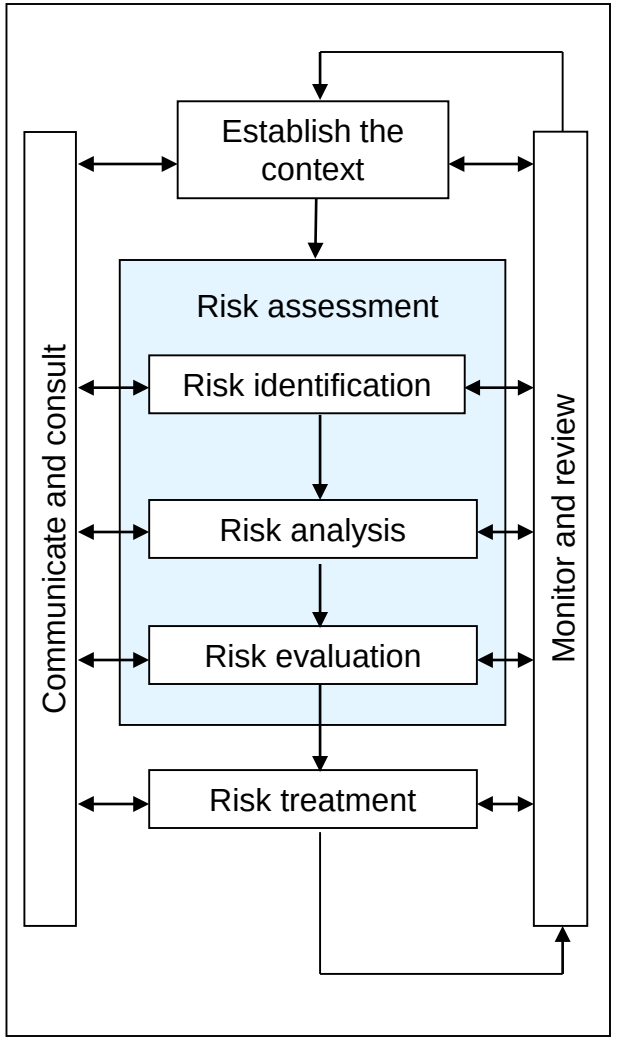
Based upon a model of continual improvement, the framework is what will *sustain* your risk management efforts

This assures that you are consistent, *process*-focused and held accountable

Building the framework includes *planning* for implementation, monitoring & review and communication

RM Process

- 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.

ERM at ECU

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

Mission Essential Task List

(METL)

"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

GREEN: Completed
ORANGE: In-Progress/Partially Completed
BLACK: Future Action

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

ECU Top Ten Enterprise Risks

	Risk Description/Title	Major Risk Category	Previous Top Ten List?
1.	Facilities Obsolescence and Deferred Maintenance	Operational	NO
2.	Additional State Budget Cuts	Financial	YES
3.	No or Insufficient Salary Raises Over Multiple Years and Corresponding Effect on Faculty-Employee Morale	Financial	NO
4.	Potential For Losing a Significant Number of Subject Matter Experts and Senior Administrators Due to Retirement Eligibility – Succession Planning (Continuity)	Operational	YES
5.	Financial Challenges of Med School (Statutory Restrictions on Clinical Revenues & Effect of Academic/Research Expenses)	Financial	NO
6.	Data and Information Security – Vulnerability to Cyber Attacks and Potential Loss or Compromise of Sensitive Data/Information	Operational	YES
7.	Increasing Federal Requirements and Compliance Expectations During a Time of Significant Budget Cuts	Compliance	YES
8.	Continued Decline in Graduate Program Enrollment	Operational	NO
9.	Reputational Risk Associated with Media-Accelerated/Induced Negativity Related to Non-Compliance	Compliance / Reputational	NO
10.	Personnel Strain Related to Oversight and Management of Ever-Growing Spread of Projects, Activities, and Opportunities	Operational	YES

Private Sector Top Risks

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

(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

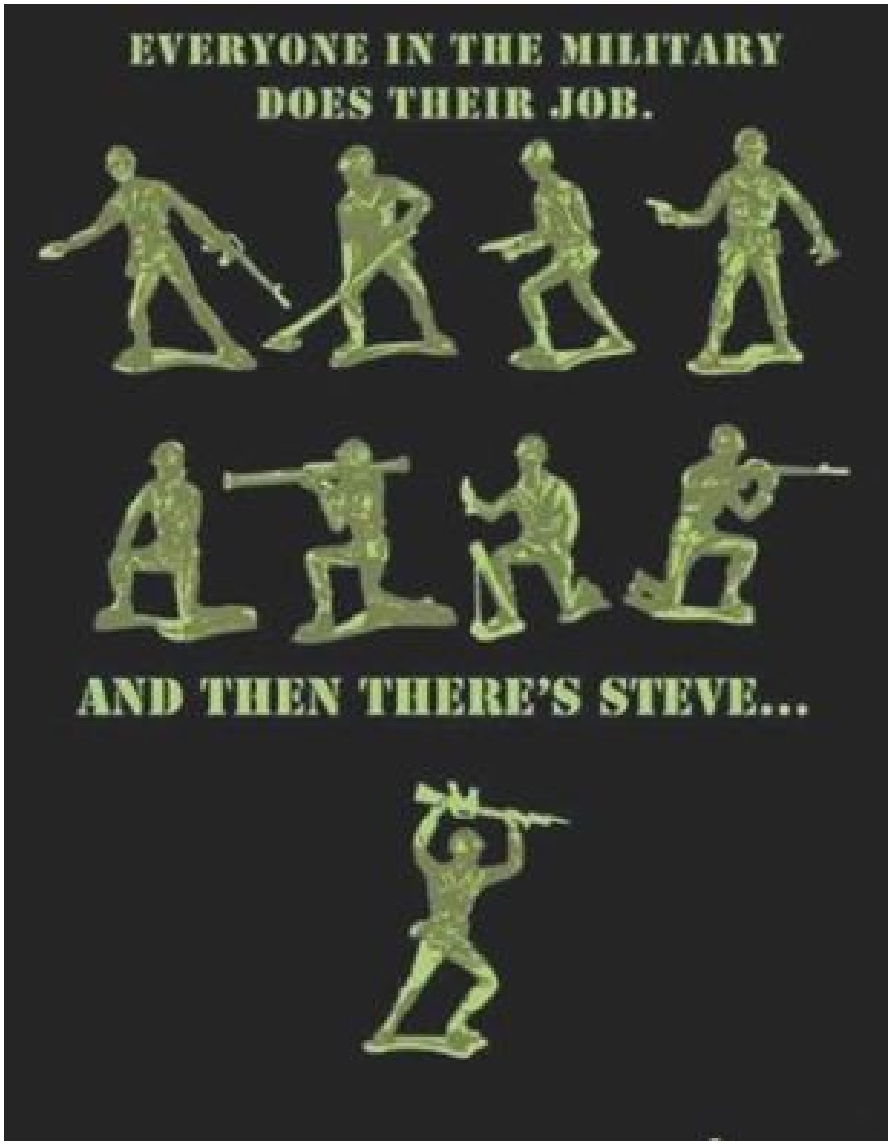
Lines of Operations

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

ERM Activities Model

Two-Year Approach

Year	Primary Activities	Focus
Even "On" Year (example: '14-'15)	• Full ERM Risk Survey • Full Risk Prioritization Exercise • Reset • Board of Trustees and Exec-Level Presentations and Involvement • Risk Management Plans Creation (or Updates)	• Engaging Key Sensors • Assessment Process (Rigor and Detail) • Risk Register Update • Fresh Look at Current and Anticipated Risk Environment
Odd "Off" Year (example: '13-'14)	• Smaller Scale Re-Prioritization/Re-Validation Exercise • Departmental Workshops • Interviews and Sensing Sessions • Presentations to Other Key Committees/Groups	• Risk Management Plans Update/Adjustment • "By Exception" Reviews • Select Risk Management Project Work • ERM "Maturity" Assessment(s) • Education


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

After-Action Review

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

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

ERM Successes

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

ERM Challenges

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

Road Ahead

ERM Program Trajectory Options





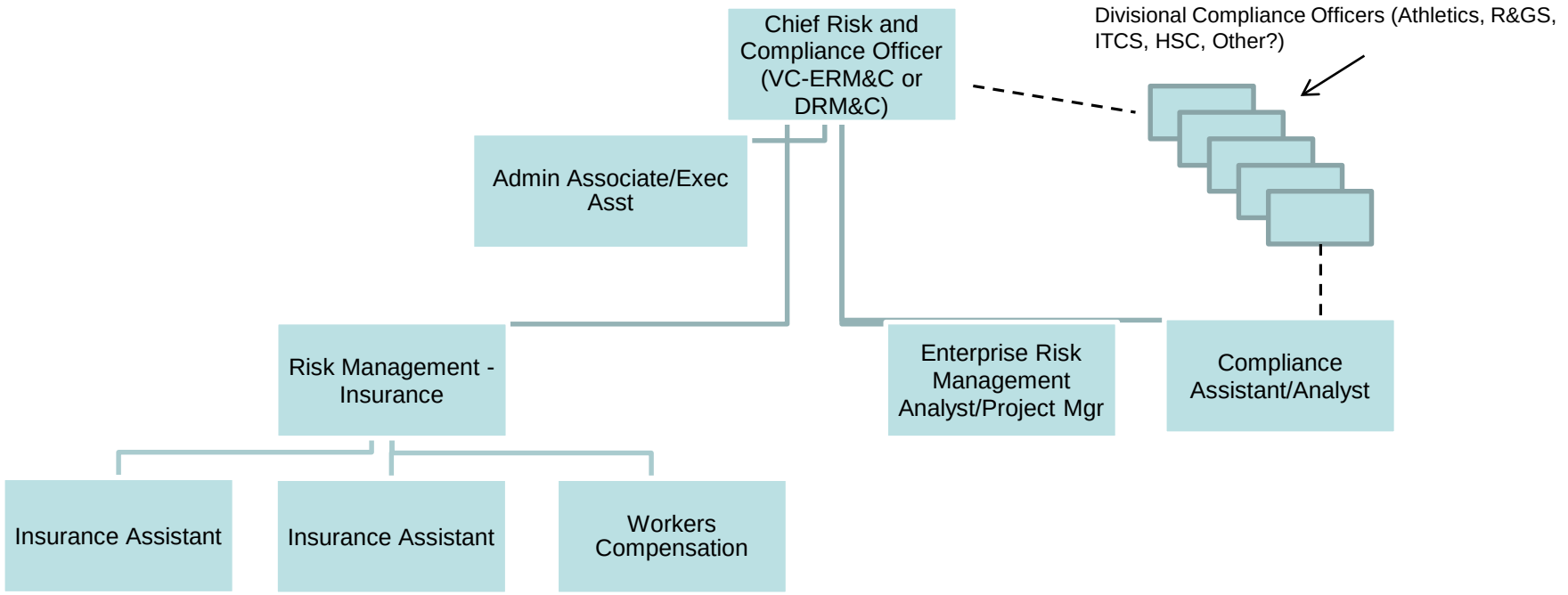
Outcomes vs. Resources

Resource Level

HIGH	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.
MOD-HIGH	Consolidated Risk Mgmt "Center of Excellence" - Under One Roof
MODERATE	ERM Integrator – Multiple Organizational Levels (Workshops, Tools, Analysis, Visibility-Enhanced)
LOW-MOD	Strategic Planning and Decision-Making Integration/ERM Best Practice Champion
LOW	Semi-Passive – Present, but Second Tier. "Bull Pen" Call up as Needed. ERM References Custodian. Risk "sensor".

Road Ahead

Notional Risk Management and Compliance Center - Institutional Level



Linus' Summary of ERM's Goal



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?

