Enterprise Risk Management – Focusing on the Right Risks

Association Conference

September 17, 2014

CliftonLarsonAllen

cliftonlarsonallen.com

Discussion Objectives

1. Discuss factors driving the need for Enterprise Risk Management

2. Learn a process for identifying, assessing and prioritizing risks

3. Share information about key items to consider for enhancing risk management in organizations

Factors Driving Organizations to Implement Enterprise Risk Management:

Why Do You Do It?

Increasing Demand for Enhanced Governance and Risk Oversight

- **2012 Dodd-Frank Act Rules**
  - compensation committee independence
  - disclosure of pay-for-performance, pay ratios, and hedging by employees and directors
  - recovery of executive compensation
  - reporting over conflict minerals essential for business
  - disclosure of government payments to resource extraction issuers, companies engaging in commercial development of oil, natural gas, and minerals
- **2010 SEC Rules to Enhance Corporate Governance Disclosures**
  - director and nominee qualifications and legal proceedings
  - diversity and director nominations
  - board leadership structure and role in risk oversight
  - accelerated disclosure of shareholder voting results
- **Rating Agencies**
  - S&P, Moody's indicate an analysis of ERM capability will be a factor in determining a company's overall credit rating
- **IT Security and Compliance**
  - Regulatory requirements, standards, and risks related to identity theft, fraud, disclosures, privacy, etc.

Board Responsibilities are Increasingly Focused on Risk Oversight

- Board fiduciary responsibilities extend beyond the traditional "hard risk" areas to include all types of risk to the organization including strategy and reputation
- Board members have a "duty of care" responsibility which includes assuring that risks are considered in decision-making and all known key risks are effectively managed

Is ERM relevant for non-profit organizations?

ERM is just as valuable to non-profits as it is to commercial/public companies

Leading practices in risk management developed in corporations can be leveraged by non-profits and associations

Every organization, regardless of type, has a need to understand risks that might impact it's ability to fulfill it's mission – no one is immune to risk.

Questions Many Organizations Are Asking

- What is our appetite for risk and what is our tolerance for deviating from expected results?
- What risks should we be focusing on? Do we know what our true top risks are?
- Once we know what the risks are, how prepared are we to address them?
- How well are we doing with the risks we are focusing on?
- Do we have a sustainable process to make risk management more than a one time event?
- How do we capture future risks and integrate them into the process?
- How aligned are we as an organization to make this happen?

What is ERM?

Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives.

- COSO Enterprise Risk Management – Integrated Framework 2004

Organizational definitions of Enterprise Risk Management (ERM) can vary widely. At its basic core, it involves having a better understanding of the risks your organization faces, and have a sustainable and repeatable process to successfully mitigate them.

Benefits of ERM

- Create a more risk aware culture
- Align risk appetite and strategy
- Enhance risk response decisions
- Minimize operational surprises and losses
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Seize opportunities
- Support cost management efforts
- Improve operational performance
- Provide better basis for allocating resources

What types of risks are Non-profit organizations focusing on?

- Many organizations are realizing that they need to focus on the full spectrum of risk categories to ensure that they have identified their true top risks, and focusing on the right things.
- Risks are specific to the particular organization but in addition to traditional risk categories such as finance, organizations may identify risks in areas such as:

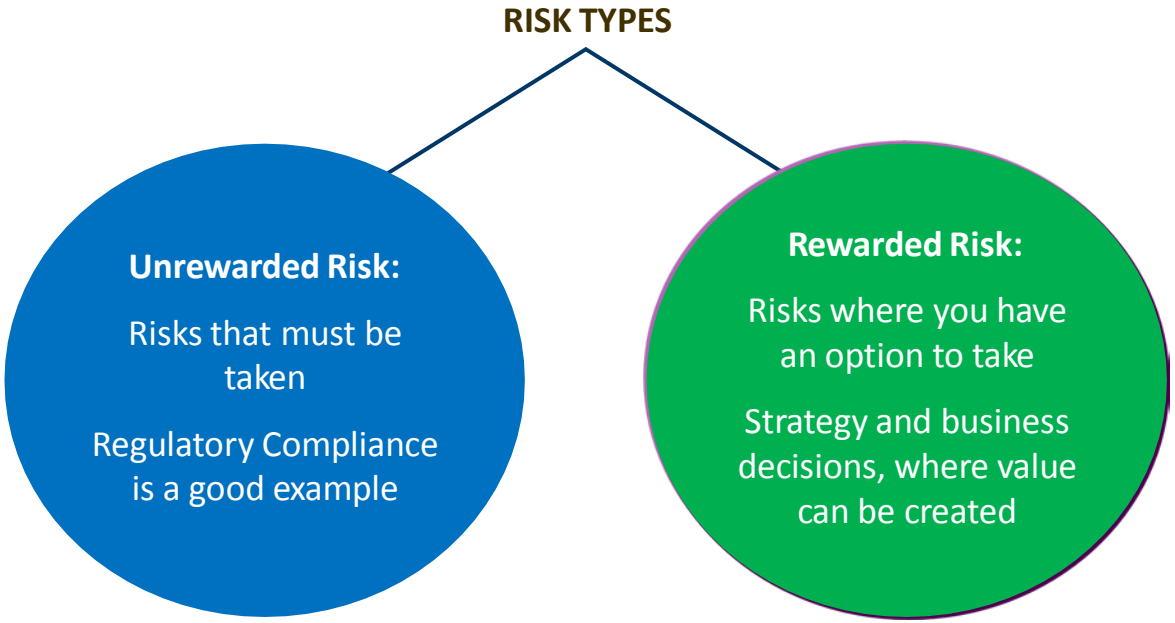
- Legislative and Regulatory change
- Economic Environment
- Vendor Management
- Human Capital Management
- Affiliated Organizations
- Business Continuity
- Medical Cost Management
- Benefit Cost Management

- Fraud
- Cyber Infrastructure
- Social Media
- Federal Regulatory Compliance
- State Regulatory Compliance
- Safety and Security
- Reputation management
- Collaboration of Care

Identifying, Assessing, and Prioritizing Risk on an Enterprise-Wide Basis :

How Do You Do It?

The Two Sides of the Risk Coin



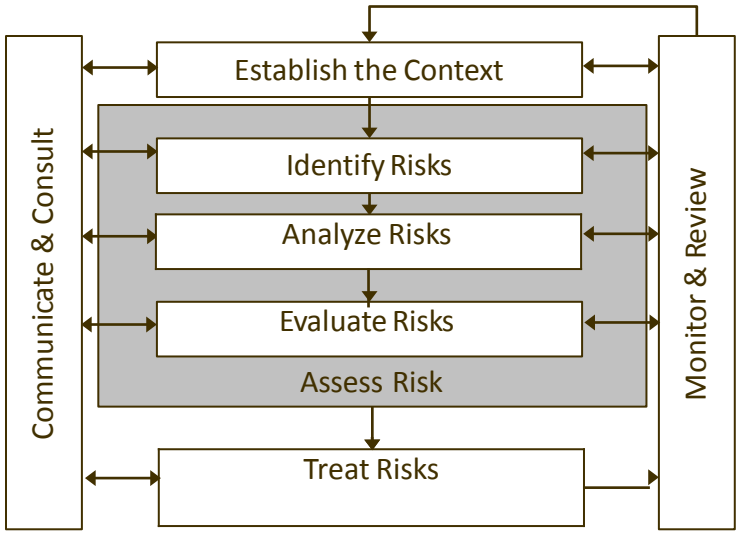
Fail to manage the Unrewarded Risks and bad things happen

Fail to take the right amount of Rewarded Risks and you don't fully reap the reward

Two Popular Risk Frameworks

COSO integrated framework

AS/NZ - ISO 31000:2009



Goals of an Enterprise Wide Risk Assessment

- An enterprise risk assessment gives organizations insight into risks in multiple categories.
- Organizations are finding that the process helps them:
  - Understand both financial and non-financial risks
  - Develop a sustainable risk assessment process you can use in future years
  - Utilize a common risk rating criteria for multiple risk types
  - Generate a prioritized risk register
  - Develop risk mitigation strategies for the key risks vs. attempting to cover all
  - Implement leading practices
  - Manage risk more effectively and efficiently
  - Develop data for board and executive risk reporting

Using a Risk "Heat Map"

The risk assessment process facilitates the identification of risks by rating the **Impact**, **Vulnerability** and **Speed of Onset**.

The overall impact of the risk can be based on multiple types of impact including:

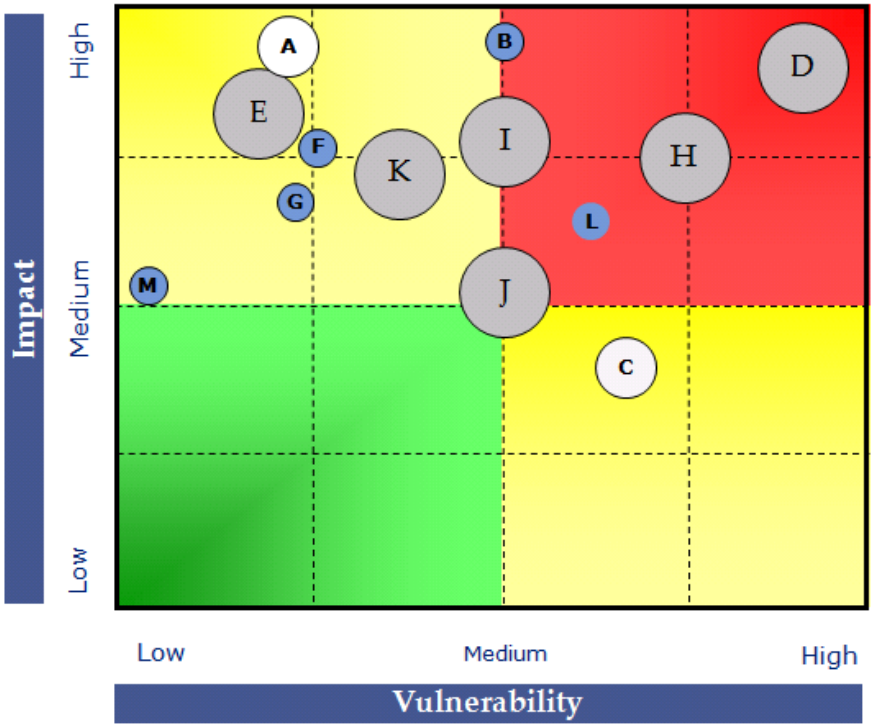
- Financial
- Reputation
- Legal/Regulatory
- Customers
- Employees
- Operations

The overall vulnerability of the risk can be based on factors such as :

- Existing controls and mitigation efforts
- Risk management capability
- Prior risk experience

Speed of Onset is based on how quickly

- the risk could occur



Example of a Basic Risk Report

Risk Description	Risk Direction	Risk Response Status	Risk Owner	Status of Additional Risk Management Activities Initiated
Failure to comply with Federal regulatory standards	→		Mr. Avoid	• Performing review of last 12 months of adverse compliance • Developing action plans for key trend areas identified from the review
Inaccurate billing for services	↘		Ms. Accept	• Assess customer concerns • Measure customer satisfaction
Insufficient business continuity planning	→		Mr. Reduce	• A project has been initiated to develop appropriate business continuity plans for all major operations and facilities.
Inadequate IT backup and disaster recovery processes	↗		Ms. Transfer	• Key steps have been completed to improve IT BCM: consolidated and improved the data center, documented processes, and retrained personnel.

Planning the ERM Journey:

Key items to consider

Evaluating Risk Management Capability

2 Key Questions on Risk Management Capabilities

Where is your organization in terms of risk management capabilities?

Where do you need (or want) to be?

Many organizations are assessing their current risk management state and setting goals for their next ERM milestone.

Key Challenges and Obstacles

ERM is usually focused on corporate objectives and corporate strategies.

Does your organization define these? Many organizations or associations often have specific missions, as well as election or appointment cycles related to board members– which may require a different perspective on assessing risks against long term objectives/strategies.

Are there other methods or models to apply?

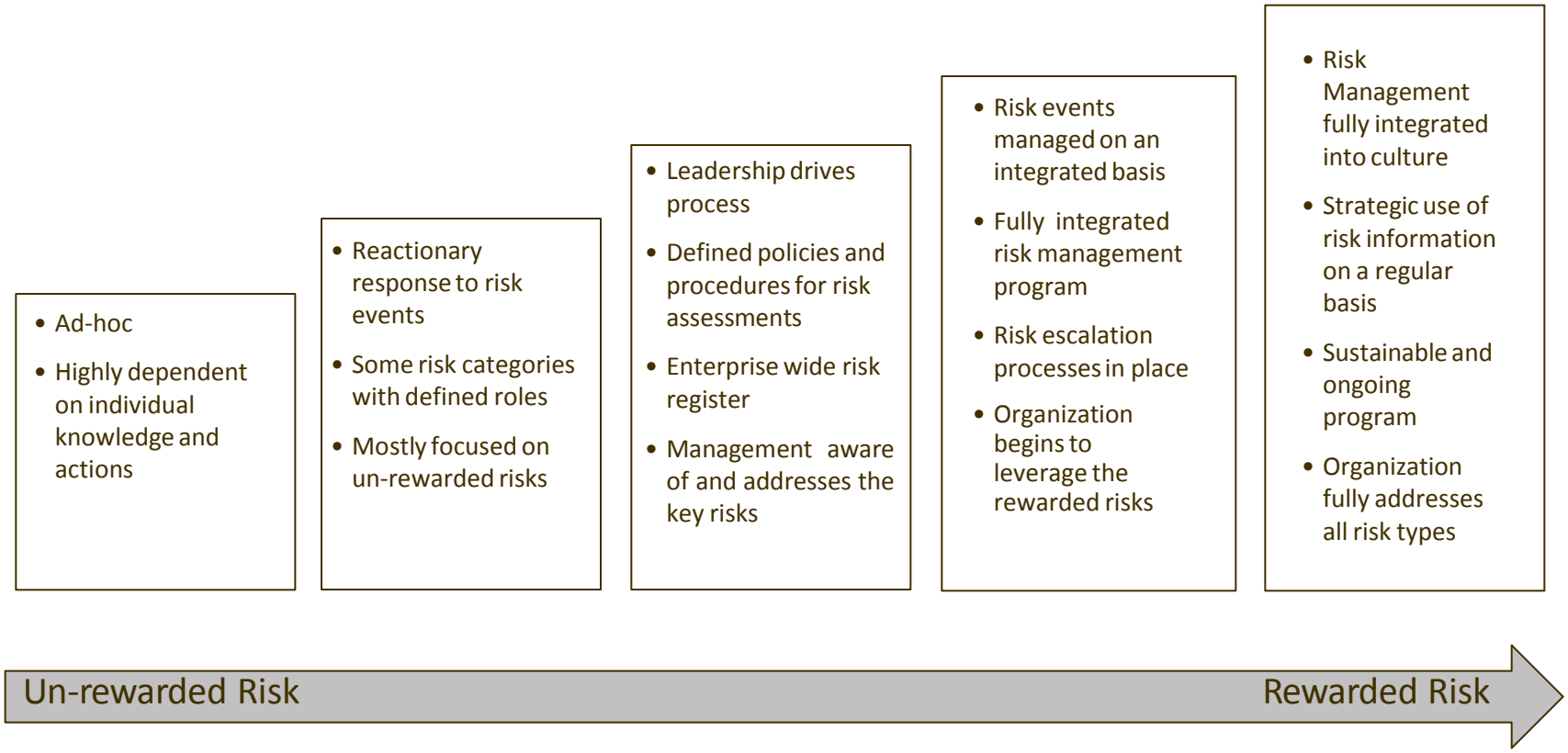
What levels of the organization are targeted?

For your organization, can "enterprise –wide" be realized?
If deployed at the department or business unit level, is there a risk of inconsistent models or assessments of risk?
What implications does this have on risk, investment, and budget/resource decisions?

How is the framework and program deployed? Corporations often assign an overall Chief Risk Officer, Compliance Officer, and/or ERM Director. Do non-profits have an entity wide equivalent?

Who would own ERM in the organization?
What about assessments or integration with other key stakeholders, departments, etc.?

The ERM Journey



Illustrative Roles and Responsibilities

Group	Responsibility
Board / Audit Committee	• Establish risk appetite • Review enterprise risks • Set the Tone at the Top
Executive Management **(Can be supported by ERM executive committee or similar group)**	• Set risk policies • Ensure policies and procedures are followed • Ensure proper resources are assigned • Serve as primary point for coordination of all enterprise risk data
ERM Function	• Provide ERM support to Executive Management and the Board • Perform overall ERM program management • Implement and Coordinate ERM processes and procedures
Business Units	• Identify and assess risks • Develop risk mitigation strategies • Monitor risks and escalate when required
Internal Audit Function	• Work with ERM function to coordinate and facilitate ERM program • Review of effectiveness of risk mitigation efforts • Provide assurance to management and board on risk exposure

Summary

- ❑ What is ERM?
- ❑ How does ERM apply to your organization, and what benefits can be derived?
- ❑ What frameworks, tools, and methodologies are most applicable?
- ❑ Challenges exist – how will your organization approach these challenges?
- ❑ What skills and capabilities current exist for risk management within your organization?
- ❑ Where to begin?
  - ✓ Seek executive "buy-in"
  - ✓ Leverage existing practices
  - ✓ "Start Small" – pilot opportunities, focus on a narrow universe of key risks, stages, etc.
  - ✓ Establish metrics and monitoring structures for accountability and sustainability

Jim Kreiser, CISA, CRMA, CFSA
Principal, IT and Risk Management Services
James.Kreiser@CLAconnect.com
717-558-0860