Enterprise Risk Management (ERM) Assessments

Issues/Concerns-
Summary and Elements to Consider
Agenda

• Introductions
• About Enterprise Risk Management, Inc.
• Topic 1: Current Issues and Concerns facing organizations
• Topic 2: Value, Framework of E.R.M. (Risk Management)
• Topic 3: Major Elements of ERM; Key Definitions
• Topic 4: Responsibility & Risk Models
• Topic 5: Proactive Strategies to evaluate an ERM program
• Why Enterprise Risk Management, Inc.
• Open Discussion
About the Company

Company Background

- Founded in 1998
- 8(A) Economically Disadvantaged Woman Owned Small Business (EDWOSB)
- GSA Schedules: MOBIS 874, Schedule 70, GSA FABS 520
- WBENC Certified Woman Owned Business
- Hispanic American Minority Owned Business
- SBD Certified Micro/Small Enterprise
- SBD/FDOT Certified Disadvantage Business Enterprise

Market Presence

- More than 130 clients
- Large and complex domestic and international clients
- Offices in:
  - Miami
  - Tampa
  - Washington DC
  - India
About the Company

Capabilities

- Cyber Security
- Risk Management
- Information Assurance
- Strategic Governance
- Regulatory Compliance
- Assurance and Attestation
- IT Audit & Advisory
- Fraud and IT Forensics
- Privacy and Consumer Protection

Sectors

- Governmental
- Financial Services
- Oil & Gas
- Energy
- Retail & Distribution
- Healthcare
- Manufacturing
- High Tech & Telecom
- Higher Ed
- Legal Services
- Hospitality
- Food, Beverage and Entertainment
- Leisure & Tourism
- High Tech

March 2013
About the Presenter

Introductions: Carlos Hondal, CPA, CFE

CMH Advisors, LLC/AFC Group, Principal/Director; 2011-Present
Advisory Service in Governance, Risk Management, Compliance, Litigation Support, and Fraud Examinations.

Ocean Bank, EVP and Chief Risk Officer; 2006-2011
Member of Mgt. Comm., CRA Comm., Technology Steering Comm., Ethics Comm. and Chairman of Mgt. Risk Committee.

Ocean Bank, SVP & Director of Audit; 1989-2006
Established Internal Audit Function, Founding member of the Audit Director’s Roundtable for the IIA Miami Chapter, Coordinated External audits & Regulatory Examinations, Lead special investigations dealing with law enforcement agencies, EDP Steering Comm., Certified Instructor in Management Training.

Coopers & Lybrand (PwC), CPA, Audit Manager; 1982-1989
Lead audits of banking, construction, retail/wholesale car dealerships and college and university projects. Also coordinated large fraud investigations and was a firm instructor for staff training “schools” as well as leading the internal quality control reviews for the Miami office of Coopers & Lybrand.
Current Issues & Concerns for most organizations in profit, non-profit, education or government (in no particular order…)

- Earnings
- Customer/Vendor complaints
- Capital Adequacy
- Credit
- Adequate Reserves
- Board of Director Supervision
- Strategic Planning
- Fraud Insider Abuse

- Cyber Security
- Compliance Issues
- Macro-economic threats
- Political Instability
- Technology threats
- Disaster Recovery Planning
- Data Privacy issues
- Etc…
Why Enterprise Risk Management (ERM)?

What specifically is ERM?

Why is ERM Important?

Why does ERM have value?

Who is responsible for ERM?
ERM Defined:

• “An ongoing process flowing through an entity or organization effected by people at every level using the company’s strategy.

• ERM is applied across every level of the organization using an entity-level, portfolio of risk.

• ERM is done to provide reasonable assurance that the entity’s management and board are geared to properly achieve their objectives in various categories or areas.”\(^1\)

1- COSO (Committee of Sponsoring Organizations of the Treadway Commission.)
ERM Framework Standards/Guidelines:

- Open Compliance & Ethics Group (OCEG) Red Book 2.0:2009 GRC Capability Model
- Sarbanes-Oxley Act of 2002 (“Sarbox”)
- Public Company Accounting Oversight Board (PCAOB)
ERM Framework Standards/Guidelines:

- Casualty Actuarial Society (2008)

- Third BASEL Accord (Basel III), Regulatory Standards to improve Capital adequacy, Stress testing and Liquidity

- Control Objectives for Information and Related Technology (COBIT), latest version, “COBIT 5” issued in 2012

- (and many others.....)
The ERM Framework

- Eight inter-related components that form the framework.

*Image Source: COSO Enterprise Risk Management Framework*
Why is ERM Important and should have value to you and your company?

• Integral part of a Company’s Corporate Governance Structure

• Strength of Internal Controls, Monitoring systems and Independent evaluation of the Risk Management System drives the success of an ERM system as well as the success of any company.

• ERM prioritizes the Time that your company should:

DEDICATE TO THE MOST IMPORTANT/IMPACTFUL ITEMS THAT PROPERLY GOVERN THE ORGANIZATION EACH DAY, EACH MONTH, EACH QUARTER AND EACH YEAR OF ITS OPERATION.
Important elements and coverage of ERM:

- Groups that must be aligned and “on the same page” for an ERM program include:
  
a. Customer Interests  
b. Shareholder/Stockholder interests and objectives  
c. Board Philosophy  
d. Management goals  
e. Legal and Regulatory responsibilities  
f. Employees/Vendors  
g. (many others, depending on your industry….)
Importance of proper, clear and consistent “Risk Language”:

- **Terminology**
- **Definitions**
- **Reporting** (challenges)
- **Scope and Audience** for risk analysis.
ERM Programs do not “FIT” all Organizations equally. Why?

- Industry Impact (inside & outside the same industry)
- “Quantitative” v. “Qualitative” environments
- Goals, Philosophy, Vision, etc….
- Micro/Macro economic and resource factors.
Classic Elements for Success in ERM:

- Proactive, not Reactive Approach (excuse the cliché !)

Comment/Observation:
If ERM is not used as a proactive management tool, by the Board and Senior Management, the ERM program will become another “Checklist to fill out.” “Remember to present and make sure it is included in the minutes of the board and management committee meeting for the audit or examination next year.”

March 2013
KEYS TO SUCCESS:

- Support from the TOP (i.e. Board & Senior Management)
- Start with small, "Foundation Building” steps
- Use existing corporate structures as much as possible
- Add to what you currently are doing to manage your risks (don’t discard the good things you do have!)
- ERM must become an essential part of your company, IN ALL RESPECTS. (“Walk the Walk”)
- Continually update and communicate success and failures to B.O.D and Sr. Management.
Major Elements of Risk (may) include:

- Market-Related Risks
- Liquidity-Related Risks
- Operational Risks ("catch-all" category)
- Strategic
- Legal
- Technological or "I.T." Risks
- Reputational

**NOTE:** other viable risk types could be and sometimes should be identified and added to this list and also tracked and managed. It solely depends on your organization.
Elements of Risks are Dependent upon:

- Industry
- Complexity of Operations
- Scope of the Products offering or market
- Financial & Geographic Diversity
QUESTION: Is Risk a BAD thing?

NO !
Risk, properly managed, should be:

- Thought of as a degree of opportunity to invest time, talent and resources in elements within a company to help it attain the organization’s goals.
- No Entity, Organization or Government Agency can make a profit or attain its goals without taking a risk.
- The Classic “risk-return” philosophy is essential in all situations, but managing that decision well to invest (or not) is what allows the philosophy to bring benefit to the Organization.
Goals are defined for this Presentation:

- Earnings
- Organic Growth
- Acquisition Growth
- Diversification
- Efficiency in Operations
- Budget vs. Actual improvements
- Patents, Breakthrough in Ideas/Technology
- Lead vs. Follow the industry (depends on philosophy)
Definitions in the ERM Framework:

- **Risk Appetite** = Amount of Risk an Entity will accept or not accept.

- **Risk Tolerance** = Threshold of Risk that the Entity can bear (“tolerate”) at a given point in time.

**NOTE**: The Board and Sr. Management will determine the risk appetite (and tolerance) of the Organization.
Establishing the correct risk appetite is critical to the success of an ERM implementation.

**Key Questions:**

- What risks will the organization not accept?
- What risks will the organization take on for new initiatives?
- What risks will the organization accept for competing objectives?
Who is Responsible for ERM?

“The Director’s major responsibility is to provide a management structure that adequately identifies, measures, controls, and monitors risk… Failure to establish a risk management structure is considered unsafe & unsound conduct.”

Key Role – Board Of Directors

• Independently pursue management on ERM strategy, plans, and performance.

• Interact with internal and external auditors to stay fully informed.

• Provide insights and inputs to management.

• Question management decisions on risks, risk treatment, and monitoring.
How do companies Track ERM and the related Risks?

- **Risk “Models”** (e.g. showing High, Medium or Low Risk) showing quantified levels of risk.
- **Risk “Dashboards”** or “Heat Maps” that graphically show the company’s risk assessment at a given point in time. These dashboards are presented periodically during the year in different levels of detail.

**Note/Comment:** The level of detail in a given “Heat Map” is relative to the reporting lines of the organization. Board-level reports are global and summarized whereas Divisional or Departmental risk reports will be more detailed and specific.
Important Concept - Qualitative (judgment) impact on Quantitative Risk Rating:

Although most risk models use quantified levels of risk (i.e. a numeric value), an important component and weight in these models is a qualitative (judgment or “gut feel”) aspect to be included in the risk assessment. Additionally, the “direction” of the risk assessment in a given risk category (e.g. increasing or stable or decreasing) is also an important consideration in the ERM process and decision-making element for an organization.
Best way to assess an ERM program? The essential characteristics:

• Active Board and Senior Management Oversight

• Adequate Policies, Procedures and Limits

• Adequate Risk Management, Monitoring and Management Information Systems.

• Comprehensive Internal Controls (without controls, risk management loses all value due to the lack of accurate and valid reporting of exposures and risks in an organization.)
Regulatory authorities that oversee organizations for financial reporting or legal purposes will evaluate the organizations relative strength of the ERM program. Some general Guidelines are as follows:

**STRONG Risk Management** – “…effectively identifies and controls all major types of risk posed by the relevant activity or function. The board and management participate in managing risk and ensure that appropriate policies and limits exist, and the board understands, reviews, and approves them.”

Regulatory authorities that oversee organizations for financial reporting or legal purposes will evaluate the organizations relative strength of the ERM program. Some general Guidelines are as follows:

ADEQUATE Risk Management – “...risk management systems, although largely effective, may be lacking to some modest degree. It reflects an ability to cope successfully with existing and foreseeable exposure that may arise in carrying out the institution’s (company’s) business plan...”

Regulatory authorities that oversee organizations for financial reporting or legal purposes will evaluate the organizations relative strength of the ERM program. Some general Guidelines are as follows:

**WEAK Risk Management**—“...risk management systems that are lacking in important ways and, therefore, are a cause for more than normal supervisory attention. The internal control system may be lacking in important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures...could have adverse effects on the safety and soundness of the financial institution (organization) or could lead to a material misstatement of its financial statements if corrective actions are not taken.”

Proactive strategies (excuse the cliché) that organizations can consider to prepare & evaluate its own ERM:

A. Governance Self-Assessment.

B. ERM Self-Assessment.

C. Specific Risk (within ERM) Assessment.

D. I.T (Technology) Self-Assessment.
Helpful Websites for you to consider and refer:

- www.coso.org
- www.aicpa.org
- www.iso.org
- www.theirm.org
- www.emrisk.com
Questions and Inquiries

For further information please contact:

**Silka Gonzalez**
*President*
CISSP, CISA, CITP, CISM, CPA
305-447-6750 (o)
sgonzalez@emrisk.com
www.emrisk.com

**Carlos Hondal**
*Principal, CMH Advisors, LLC*
CPA, CFE
chondal@emrisk.com

March 2013