The ERM Revolution: Advancing the Cause
April 26, 2017

Presented by:
Jim Yard and Don Owens
Contact Information

Donald R. Owens, Shareholder
Risk Advisory Services
CPA, CITP, CFF, CIA, CFSA, CRMA, CBA
Schneider Downs & Co., Inc.
65 E State Street, Suite 2000
Columbus, OH 43215

dowens@schneiderdowns.com
Work Phone: (614) 586-7257
Cell Phone: (614) 271-8551

James B. Yard, Shareholder
Risk Advisory Services
CPA, CIA, CISA
Schneider Downs & Co., Inc.
One PPG Place Suite 1700
Pittsburgh, PA 15222
jyard@schneiderdowns.com
Work Phone: (412) 697-5345
Cell Phone: (724) 822-3915
Disclaimer

IRS CIRCULAR 230 DISCLOSURE: Any tax advice contained in this communication (or in any attachment) is not included or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) for promoting, marketing or recommending to another party any transaction or other matter addressed in this communication (or in any attachment).

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of Schneider Downs & Co., Inc. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute accounting, tax or legal advice or create an accountant-client or attorney-client relationship.
Quotes That Apply to ERM

Not everything that counts can be counted, and not everything that can be counted counts.

Albert Einstein
Quotes That Apply to ERM

The important thing is not to stop questioning. Curiosity has its own reason for existing.

Albert Einstein
Quotes That Apply to ERM

Insanity: doing the same thing over and over again and expecting different results.

Albert Einstein
Quotes That Apply to ERM

A man should look for what is, and not for what he thinks should be.

*Albert Einstein*
Quotes That Apply to ERM

If you can't explain it simply, you don't understand it well enough.

Albert Einstein
Key Drivers of ERM

• Protection of Life and Limb
• Protection of Capital
• Maximization of Earnings
• Achievement of Strategic Objectives and Goals
• Stakeholders Expectations
• Compliance with Laws and Regulations
Key Laws and Enforcement Agencies

- Dodd-Frank Act
- Foreign Corrupt Practices Act
- Sarbanes-Oxley Act
- U.S. Federal Sentencing Guidelines
- Whistleblowers Protection Act
- Occupational Safety and Health Act
- Equal Employment Opportunity Act
- Aviation and Transportation Security Act
- Environmental Protection Act
Key Laws and Enforcement Agencies

- SEC and PCAOB
- Department of Justice
- Department of Labor
- Immigration and Customs
- Occupational Safety and Health Administration
- IRS
- FED/FDIC/OCC/NCUA/CFPB
- Environmental Protection Agency
- National Labor Relations Board
- Department of Homeland Security
Where Is Your Organization’s Weak Link In Managing Risk?
Theory of Risk Relativity
Einstein’s Theory of Relativity

Objects, moving at the speed of light, are measured differently given the proximity to the object of the one doing the measuring. This means measurement and proximity, themselves, both function to alter what is being measured.

\[ E = mc^2 \]
Theory of Risk Relativity

Risk will be measured differently within the same organization given the proximity to the risk of those doing the measuring.
Capturing and Measuring Risk
Capturing and Measuring Risk

• The concept of risk
  – is not easily quantified.
  – is not expressible in a neat, numerical package that all can understand.
  – can be highly subjective, having both qualitative and quantitative elements.
Arriving at a universal “risk formula” to apply to events, occurrences and/or opportunities is very challenging.

– TRUTH: Every organization, within and outside of a given industry, has its unique applications of risk management policies and practices.
Leading Practices of ERM

• Establish a risk management policy for your organization
• Communicate your risk management policy
• Fully engaged board of directors
• Integration of risk management into the business functions
• Risk ownership and accountability for risk management
• Transparency
Leading Practices of ERM

- Integration of risk with strategic planning
- Intelligence gathering (benchmarking, trend analysis)
- Continuous monitoring (data analytics)
- Scenario analysis (stress testing, disaster recovery)
- Consistent and continuous communication
- Allocate time and resources
Key Drivers of ERM

Risk Measurement

• Inherent and residual risk measurements (establish measurements at the company level)
  – Risk Acceptance (risks in the normal course of business)
  – Risk Appetite (determined based on strategy/long-term business plan)
  – Risk Tolerance (point at which potential impairment occurs, entering crisis mode)
ERM – Identifying the Risks

Ladies and gentlemen, this is your captain speaking. There is a minor malfunction in the pressurization system, but no problem, an oxygen mask will come out of the unit above your seat automatically.
Key Drivers of ERM

Risk Attitude

• Knowledge of risk
• Commitment (lack of) to manage
• Culture of organization
Evolution of Risk Management

Traditional risk management is characterized by fragmented responsibility rather than a holistic approach encompassing the entire enterprise; a focus on discrete events; a perception of risk management being a product of transaction (insurance) or a reaction to events.

The move to today’s ERM is strategic and focused. Today’s ERM model allows organizations to integrate business managers with risk managers, increase non-financial risk awareness, and increase involvement from all areas of the organization – executive management, board members, and business.
When it comes to ERM, being proactive is the only course of action.
ERM Pitfalls

- Not linking strategic planning and risk management
- Not positioning ERM as a management practice
- Procedural approach (restrictive/limiting)
- Many failures explained by challenges of responding to a “Black Swan” event
- Diminishing transparency
- Lack of support at the executive level
ERM Pitfalls (cont.)

• Pitfalls
  – Competing priorities of ERM staff
  – Placing risk management oversight with the audit committee
  – Not looking beyond impact and likelihood
  – Lack of understanding on the “Big Bets” being taken
  – Failure to assess industry and peer dynamics
ERM Principles

• ERM should:
  – Be linked and embedded in your strategy
  – Create and protect value
  – Be part of all processes
  – Be part of your decision making
  – Be used to handle uncertainty
  – Be systematic and timely
ERM Principles (cont.)

• ERM should:
  – Be based on the best data
  – Be tailored to your environment
  – Consider human factors
  – Be transparent and inclusive
  – Be responsive and iterative
  – Support continual improvement
Traditionally, risk was viewed more from a financial risk perspective. The new standard is to look at risk throughout the enterprise.
ERM – Technology

Traditional vs. Leading Edge Technology

Privacy and Security
Social Media and Networking
Mobile Devices
Malware and Viruses
Spam, Scams and Phishing
Corporate Espionage
Regulatory (ERM)
Cloud Computing
Hardware and Software Failure
ERM – Embracing Analytics

DATA and the Digital World:
• Continuous monitoring of key risk indicators
• Quantifiable risk measurements
• Ability to assess entire populations
• Create risk dashboards

Challenges:
• Technology and talent
• Quality of data and its availability
• Access to comparable external data sources
Information = Expectations

Expectations = Perceived Pattern/Outcome

Perceived Pattern/Outcome = Data Analytics

Data Analytics = Information
Rating Risks

Traditional Risk Rating:
- Probability
- Severity

Expansive Risk Rating:
- Probability/likelihood/Vulnerability – risk threat level absence controls
- Impact/Severity/Loss Magnitude – measurements include financial, threat to human life, environmental, etc.
  - Also consider future repercussions/secondary effects (prime effects and the secondary effects ... quake/aftershocks/longer term ramifications)
Rating Risks (cont.)

Expansive Risk Rating (cont.):

- Velocity/speed – speed at which the risk occurs, and will management have sufficient opportunity to react to its onset
- Frequency/Persistence – one-time event or recurring and at what rate
- Direction of risk/threat
ERM Conceptually
Three Lines of Defense

The Three Lines of Defense Model

Senior Management

1st Line of Defense
Management Controls
Internal Control Measures

2nd Line of Defense
Financial Control
Security
Risk Management
Quality
Inspection
Compliance

3rd Line of Defense
Internal Audit

Governing Body / Board / Audit Committee

External audit
Regulator

Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41
ERM is a Continuous Process

Risk Qualitative and Quantitative Techniques

**QUALITATIVE:**
- Risk identification
- Risk rankings
- Risk maps
- Risk maps with impact and likelihood
- Risks mapped to objectives or divisions
- Identification of risk correlations

**QUALITATIVE/QUANTITATIVE:**
- Validation of risk impact
- Validation of risk likelihood
- Validation of correlations
- Risk corrected revenues
  - Gain/loss
  - Tornado charts
  - Scenario analysis
  - Benchmarking
  - Net present value
  - Traditional measures

**QUANTITATIVE:**
- Probabilistic techniques:
  - Cashflow at risk
  - Earnings at risk
  - Earnings distributions
  - EPS distributions

LEVEL OF DIFFICULTY AND AMOUNT OF DATA REQUIRED
Cost Benefit of Risk Management

Where do we want to go?

Objectives

How well do we achieve our objectives?

Performance

What can go wrong?

Risks

How can we ensure that we will achieve all our objectives?

Controls
Takeaways...

• There is not a uniform definition of risk.
• We view risk differently (proximity).
• Attempting to quantify (dollar amount to future contingency) risk is an ever changing dynamic as risk is a subjective (attitudes define it) phenomenon (risk is not stable) that is always changing (impact).
Takeaways...

- Risk itself is constantly changing and at the same time, so are attitudes about risk.
- Objective and subjective measurements of risk are continually interacting, leaving measurement of risk challenging.
As one of the largest certified public accounting and business advisory firms in the region, Schneider Downs serves clients throughout the country and around the world. By integrating high-quality resources, systems and personnel, Schneider Downs has built a reputation of delivering individualized services built on insight, innovation, and experience to meet each client’s specific needs.

For more information, visit us at www.schneiderdowns.com