THE HIGH COST OF “ERM HERD MENTALITY”
ERM WRONG TURNS & THE WAY FORWARD

TIM LEECH, MANAGING DIRECTOR GLOBAL SERVICES
RISK OVERSIGHT INC. (WWW.RISKOVERSIGHT.CA)

September 11, 2012
Your Presenter

Tim Leech
Managing Director Global Services
Risk Oversight Inc.
www.riskoversight.ca
tim.leech@riskoversight.ca
Agenda

• ERM Globally & Herd Mentality
• ERM Scorecard
• ERM Herd Mentality Wrong Turns
• Recommendations for ERM Herd Leaders
• Demand Driven/Objective Centric – What is it?
• Supply Driven/Risk & Control Centric – What is it?
• Business case for change
• IIA/RO Training Opportunities
• Questions
450 sheep jump to their deaths in Turkey

ISTANBUL, Turkey (AP) — First one sheep jumped to its death. Then stunned Turkish shepherds, who had left the herd to graze while they had breakfast, watched as nearly 1,500 others followed, each leaping off the same cliff, Turkish media reported.

In the end, 450 dead animals lay on top of one another in a billowy white pile, the Aksam newspaper said. Those who jumped later were saved as the pile got higher and the fall more cushioned, Aksam reported.

The estimated loss to families in the town of Gevas, located in Van province in eastern Turkey, tops $100,000, a significant amount of money in a country where average GDP per head is around $2,700.

ERM Globally & Herd Mentality

Definition of Herd Mentality:

The term herd mentality is the word herd, meaning "group of animals," and mentality, implying a certain frame of mind. However the most succinct definition would be: “How large numbers of people act in the same ways at the same times.” Herd behavior is distinguished from herd mentality because it applies to all animals, whereas the term mentality implies a uniquely human phenomenon.

**Herd mentality implies a fear-based reaction to peer pressure which makes individuals act in order to avoid feeling "left behind" from the group. Herd mentality is also sometimes known as "mob mentality."**

ERM Globally & Herd Mentality

ERM Herd Mentality Leaders:

- COSO
- SEC/PCAOB/Securities regulators globally
- IIA/RMA/RIMS/GARP/PRIMIA/FEI/AICPA
- Bank regulators/Basel guidance
- ISO 31000/AS/NZ 4360
- Consulting firms
- ERM/GRC software vendors
ERM Scorecard

The truth is that a large % of ERM initiatives have failed badly or sub-optimized.

Few meet board risk oversight criteria established by the NACD Blue Ribbon Commission “Risk Governance: Balancing Risk and Reward”
ERM Scorecard

2008 Global Financial Crisis –

Weak risk management and oversight identified as a root cause of the crisis. But most had some form of ERM. Senior Supervisors Group study identified the following root causes in failed institutions:

• the failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm;

• compensation programs that conflicted with the control objectives of the firm;

• inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and

• institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel.

Polling Question #1

1. Which of the following was not identified by commissions as one of the root causes of the 2008 global financial crisis:
   a) Deficient board oversight of risk
   b) Deficient board oversight of risk appetite/tolerance
   c) Deficient internal audit capability and processes
   d) Misaligned reward systems
   e) Don’t know

ERM Scorecard

Limited True Adoption by Senior Executives and Boards

Current Stage of ERM

- 36%: There is no structured process for identifying and reporting top risk exposures to the board.
- 28.2%: Mostly track risks by individual silos of risk, with minimal reporting of aggregate top risk exposures to the board.
- 23.3%: Mostly informal and unstructured, with ad hoc reporting of aggregate top risk exposures to the board.
- 12.5%: Systematic, robust and repeatable process with regular reporting of aggregate top risk exposures to board.

ERM Scorecard

COSO 2010 study disclosed that a large % of ERM initiatives were not delivering to a “significant or a great deal” key benefits promised by ERM promoters.

ERM Scorecard

In Summary:

ERM implementations to date have not delivered promised benefits in a large percentage of organizations around the world; and failed in a spectacular way in dozens of the world’s largest and previously respected organizations.
WRONG TURN #1 –
Missing Focus on Objectives (ISO)

ISO 31000 doesn’t stress the need for clear linkage to objectives assessed or the impact on risk of missing/unclear/vague/poorly constructed objectives. This is somewhat puzzling given the ISO 31000 definition of “risk” is:

2.1
risk
Effect of uncertainty on objectives

ERM Herd Mentality Wrong Turns

WRONG TURN #2 –
Missing Focus on Objectives (COSO)

COSO decided in 1992 that setting and communicating objectives isn’t part of an integrated control framework:

*The “objectives” component has been eliminated as a separate component. The view expressed by some respondents that the establishment of objectives is part of the management process but is not part of internal control, was adopted. The final report recognizes this distinction, and discusses objective setting as a precondition to internal control.*

ERM Herd Mentality Wrong Turns

WRONG TURN #3 –
Focusing on Risks One by One

Most objectives are affected by multiple risks that are often interconnected. ERM approaches that emphasize “risk registers”, “risk owners” and “heat maps” often ignore this fundamental truth, resulting in unreliable risk assessments.
ERM Herd Mentality Wrong Turns

WRONG TURN #4 –
Making “Risk Registers” King
ERMS Herd Mentality Wrong Turns

WRONG TURN #5 – Falling in Love with “Heat Maps”
WRONG TURN #6 – Ignoring “Black Swans”

"Black swan management" is a term coined by Oxford University professor Bent Flyvbjerg in 2010 in his course on major program risk at Oxford.[1] The concept was later used in an article in Harvard Business Review.[2] Black swan management is based on Nassim Taleb's idea of the black swan, defined as an event that has low probability but causes massive consequences.
WRONG TURN #7–
Focusing on “controls” … not broader “risk treatments”

control (kn-trl) tr.v. controlled, controlling, controls

1. To exercise authoritative or dominating influence over; direct.
   See Synonyms at conduct.
2. To adjust to a requirement; regulate: controlled trading on the stock market;
   controls the flow of water.
3. To hold in restraint; check: struggled to control my temper.

Source: The Free Dictionary

ERM Herd Mentality Wrong Turns

WRONG TURN #7 (continued)—
Disproportionate focus on testing “controls” and limited attention to identifying and measuring risks that create uncertainty and risk status

Example: PCAOB Auditing Standard #5 for SOX 404 (b)
949 instances of the word “control”
193 instances of the word “risk”
0 instances of the words “risk treatment”
0 instances of the words “risk mitigation”
0 instances of the words “risk acceptance”
0 instances of the words “risk avoidance”
ERM Herd Mentality Wrong Turns

WRONG TURN #8– Mandating the use of a “control effectiveness” not “risk effectiveness” opinions” for SOX 404
ERM Herd Mentality Wrong Turns

WRONG TURN #9–
Requiring/using flawed/unproven assessment frameworks like COSO 1992/COSO 2013

Unfortunately, to date, no research has ever been done that validates the premise that organizations that manifest the attributes of any of these frameworks actually have better internal control than those that don’t.

Of equal interest, no effort has ever been undertaken to determine if COSO 92 is superior to CoCo or Cadbury, or more contemporary governance risk and compliance frameworks like the OCEG Red Book GRC Maturity Framework, as a predictive tool for control effectiveness opinions.

ERM Herd Mentality Wrong Turns

WRONG TURN #10–
Not practicing what you preach… no risk assessment

Risks to the objective of successful ERM implementation:

1. Don’t know if ERM is actually producing the desired results/benefits/don’t measure success.

2. Senior executives and boards unwilling to use formal risk assessment methods and tools on really important business objectives like acquisitions and major investments as they don’t accept it really adds value. This message is communicated to all those below them.

3. Senior executives and boards refuse to use formal risk assessment as a core element of strategic planning and budgeting as they don’t buy the premise that it will help.

4. Authoritative groups, including the SEC in the U.S., CSA in Canada, and security regulators around the world, still do not accept that ERM should be used for the objective of producing reliable external financial disclosures. (NOTE: The refusal of the SEC to accept ISO 31000 compliant assessment methods means two separate data/software frameworks must be maintained. One for ERM work and one for process/control centric SOX 404 assessment work)
ERM Herd Mentality Wrong Turns

PERHAPS THE BIGGEST & MOST SENSITIVE WRONG TURN

The internal audit profession has not recognized the debilitating conflict between traditional direct report internal audit (i.e. IA is primary risk and control analyst/reporter) and what needs to happen to lay a foundation for effective and embedded ERM (i.e. management is primary risk and control analyst/reporter) and, most importantly, what IA needs to do differently to help enable successful and effective ERM.
Polling Question #2

What is the primary reason you think thousands of ERM initiatives have failed globally?

a) Not enough management incentives.
b) Boards of directors are OK with status quo.
c) Internal and external audit processes continue to focus on providing subjective opinions on “control effectiveness”, not quality assuring management reports on the current residual risk status/composite uncertainty related to important objectives.
d) ERM processes have fixated on analyzing individual risks, not providing useful information on the certainty/uncertainty of achieving key objectives linked to value creation/value erosion.
e) All of the above
f) Don’t know
Recommendations for ERM Herd Leaders

Risk Oversight white paper THE HIGH COST OF ERM HERD MENTALITY (www.riskoversight.ca) proposes specific recommendations for:

- SEC, PCAOB & REGULATORS
- COSO
- IIA
- ISO
- CORPORATE ERM SPONSORS

NOTE: The Chair of COSO publicly announced in June 2012 that they will not accept recommendations made by respondents to the 2011 exposure draft to integrate the COSO ERM framework with the integrated control framework in COSO 2013
Demand Driven/Objective Centric ERM – What is it?

Demand Driven ERM Defined:

Boards of directors and senior management demand and receive reliable information on the true residual risk status on all objectives necessary for success of the organization – in essence, composite uncertainty ratings on a universe of key end result business objectives.

The overarching goal is **consensus agreement on the acceptability of the organization’s residual risk status**, including risk appetite and tolerance, related to key strategic value creation/value erosion linked objectives up to and including the board of directors.
Demand Driven/Objective Centric ERM – What is it?

Demand Driven ERM Defined:

While risk oversight objectives may vary from company to company, every board should be certain that:

1. the risk management system informs the board of the major risks facing the company
2. an appropriate culture of risk-awareness exists throughout the organization
3. there is recognition that management of risk is essential to the successful execution of the company’s strategy

Demand Driven/Objective Centric ERM – What is it?

Demand Driven ERM Defined:

While risk oversight objectives may vary from company to company, every board should be certain that:

4. the risk appetite implicit in the company’s business model, strategy, and execution is appropriate
5. the expected risks are commensurate with the expected rewards
6. management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company’s business model and strategy

Demand Driven/Objective Centric ERM – What is it?

Objective Centric ERM Defined - Key Attributes:

1. Risks only truly exist in the context of one or more implicit or explicit objectives. This interpretation is consistent with the ISO 31000 definition of “risk” – If there are no objective(s)/no risks

2. Objectives should be “end result objectives” - not “how to’s”

3. Clear and specific end result objectives enable better risk assessments relative to situations where objectives are implicit, non-existent and/or vague

4. Objectives are impacted by multiple risks that create uncertainty related to the achievement of the objective(s)
Demand Driven/Objective Centric ERM – What is it?

Objective Centric ERM Defined - Key Attributes:

5. Objectives should have an “Owner/Sponsor.” They have primary responsibility for deciding on risk assessment rigor levels and reporting upwards in the organization on residual risk status. This is another key element of “demand driven.”

6. Users, including the board of directors, need information to evaluate the composite uncertainty of achieving objectives, the potential impact(s) of that uncertainty, current performance data including how it relates to others, and any impediments in the way of adjusting residual risk status. This principle could be applied to all facets of an organization including the reliability of external financial disclosures.
Demand Driven/Objective Centric ERM – What is it?

Objective Centric ERM Defined - Key Differentiators:

• Use of an OBJECTIVE REGISTER versus Risk Register. Owners may still be defined and assigned for risks and risk treatments at the discretion of the OBJECTIVE OWNER/SPONSOR.

• Composite picture of RESIDUAL RISK STATUS linked to objectives including “concerns” created by plausible risks with no risk treatment of partial risks treatment, objective performance information, impact of non or partial achievement of objective(s), and impediment information.

• A composite rating on residual risk status that the OWNER/SPONSOR must assign and take responsibility for. A Residual Risk Status rating of 0 means Owner/Sponsor believes RESIDUAL RISK STATUS is within organization’s risk appetite. (NOTE: This can include significant levels of residual risk.) Higher RRS ratings denote the level of escalation for review of the RESIDUAL RISK STATUS in the organization.
Demand Driven/Objective Centric ERM – What is it?

Objective-Centric Risk Assessment and Ratings:

RESIDUAL RISK RATING DEFINITIONS

0 Fully Acceptable – Residual risk status is acceptable. No changes to risk treatment strategy required.
1 Low – Inaction on unacceptable terms could result in very minor negative impacts. Ad hoc attention may be required to adjust status to an acceptable level.
2 Minor – Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust status to an acceptable level.
3 Moderate – Inaction on unacceptable risk status could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust status to an acceptable level.
4 Advanced – Inaction or unacceptable risk status could allow continuation of or exposure to serious negative impacts. Senior management attention required to adjust risk status.
5 Significant - Inaction on unacceptable risk status could result in or allow continuation of very serious negative impacts. Attention required to adjust status to an acceptable level.
6 Major – Inaction on unacceptable risk status could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.
7 Critical - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.
8 Severe - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very severe negative impacts. Senior board level attention urgently required.
9 Catastrophic - Inaction on unacceptable risk status could result in or allow the continuation of catastrophic proportion impacts. Senior board level attention urgently required to avert a catastrophic negative impact on the organization.
10 Terminal - The current risk status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from the board and senior management to prevent the demise of the entity.
Demand Driven/Objective Centric ERM – What is it?

Objective Centric ERM Defined - Key Differentiators:

- Specific step asking OWNER/SPONSOR to assess whether RISK TREATMENT STRATEGY is “Optimized”.

- OWNER/SPONSOR has primary responsibility to decide level of risk assessment rigor/rigour warranted. This can range from “quick and dirty” to very sophisticated using the full range of risk assessment tools. (e.g. risk velocity estimates, KRI$s, risk escalation triggers, Monte Carlo simulations, etc)

- RISK TREATMENT documentation includes details on RISK SHARING, RISK FINANCING, RISK TRANSFER and RISK MITIGATION. RISK MITIGATION information differentiates whether it is mitigating likelihood only, consequence only, or both.
Supply Driven/Risk & Control Centric
What is it?

• Simply defined, it is the assurance approach used by the majority of organizations in the world today.
• IA performs “direct report audits” focused on forming subjective opinions on control adequacy, not identifying the current residual risk status related to key objectives or quality assuring management representations.
• Management is not formally responsible for analyzing and reporting upwards on residual risk status related to key objectives.
• Assurance is “supply driven” by silo assurance providers including IA, ERM specialists, safety, environment, compliance and others.
• ERM is not integrated in any real positive way with the direct report internal audit work focused on providing control effectiveness opinions.
• ERM initiatives are “risk centric” not objective centric and are supply driven by one or more staff functions.
Polling Question #3

3. Which of the following is NOT a core element of Demand Driven/Objective Centric ERM/assurance?
   a) Establishing clarity on the role of the board of directors to oversee risk management processes and management’s risk appetite/tolerance.
   b) Creating and regularly updating information on the organization’s residual risk status related to key strategic objectives and objectives linked to major value eroding risks.
   c) Completing annual audit plans and providing IA opinions on control effectiveness on a small percentage of the assurance universe.
   d) Assigning primary responsibility to Owner/Sponsors to report upwards on residual risk related to business objectives.
   e) Don’t know
1. Traditional “risk centric” ERM methods and IA have a high failure rate and have frequently missed major risks.

2. Many boards and senior executives do not currently see ERM or IA as a tool to increase certainty / reduce uncertainty related to the achievement of business objectives, but rather see it as a compliance exercise.

3. Many “risk centric” ERM approaches become a compliance exercise focusing on updating the organization’s risk register once a year or once a quarter.

4. Risk centric approaches to ERM do not identify the relationship between current risk treatment strategies and current performance levels on achieving objectives. This reduces the motivation of managers and work units to see value in ERM and allows sub-optimal risk treatment strategies to remain in place.

5. Assigning “owners” to risks that link to objectives that have no owner/sponsor isn’t logical.
5. Regulators claim they want evidence of more effective risk management and risk oversight processes. Calling for more of what hasn’t worked well in the past called “ERM” isn’t the solution.

6. Risk centric approaches to ERM do not include guidance on where and how much ERM rigor should be applied; or how to assess whether current risk treatment strategies in place are “optimized”, i.e. the lowest possible cost capable of producing acceptable residual risk status.

8. Commissions around the world have identified misaligned reward systems as a root cause of many massive governance failures including the 2008 global financial crisis. Separating risks from objectives and assigning owners to risks but not assigning owners to objectives makes aligning risk management and performance management significantly more difficult.

9. Some commissions are recognizing the need for clear linkage to objectives in risk assessment processes and the need to measure performance. The King III work in South Africa is an example.
10. Ignoring the well known adage “If you keep doing what you've always done - you'll keep getting what you've always gotten” is a risk the world shouldn’t ignore.
Polling Question #4

4. In your opinion, which of the following is the #1 reason internal audit departments should champion demand driven/objective centric assurance?
   a) Boards will expect IA to help them meet emerging risk oversight expectations
   b) IA is currently not seen as playing a key role helping organizations achieve key strategic objectives – this would help
   c) It will refocus IA on the full range of possible “risk treatments” not just “controls”
   d) It will simply work better than status quo assurance approaches and better help organizations achieve key objectives and avoid disasters
   e) If IA doesn’t provide the information boards need to meet new risk oversight responsibilities others will
   f) All of the above
   g) Don’t know
IIA/RO Training Opportunities

• IIA Toronto and Risk Oversight will be offering “Core Risk Management Skills for Auditors and Facilitators” Sept 24-25, 2012. For more information see: http://bit.ly/RozFt8

Questions???

Tim Leech

tim.leech@riskoversight.ca
www.riskoversight.ca

Twitter: www.twitter.com/riskoversight