Enterprise Risk Management in the Oil & Gas Industry

William A. Sherwood
Gordon, Arata, McCollam, Duplantis & Eagan LLC
1980 Post Oak Boulevard, Suite 1800
Houston, Texas 77056
(713) 333-5500 – Telephone
(713) 333-5501 – Fax
bsherwood@gordonarata.com
www. gordonarata.com

GORDON ARATA MCCOLLAM DUPLANTIS & EAGAN, LLC SEMINAR

JULY 31, 2013

-

© All Rights Reserved

TABLE OF CONTENTS

I. INTRODUCTION

Enterprise Risk Management ("ERM") is balance sheet protection. Its essential goal is to avoid the destruction of core value. A residual benefit is the expansion of opportunity.

Few "experts" in the mid-1980's anticipated or expected the demise of the Soviet Union or the implosion of the Berlin Wall, events which occurred only a few years later. And yet, with the benefit of hindsight, these events seem predictable, even pre-ordained and inevitable. The experts had a confidence, which was probably reliable in the ordinary circumstance, but which proved undeserved when revolutionary currents would disrupt the status quo.

Or, in the oil and gas industry, unforeseen dysfunctions and concatenations can cascade into a catastrophe, which no one has predicted, or feared.

Many settings demonstrate the limitations inherent in a prospective analysis of risk.

> "… the [current economic] crisis has been compounded by the banks' so-called risk-management models, which increased their exposure to risk instead of limiting it and rendered the global economic system more fragile ever."[1]

II. RISK AND LOSS

A. Risk

"Risk" is the potential that an adverse event may or may not occur.[2] Risk is inherent within every business enterprise.

> "Risk events are occurrences – catastrophic incidents caused by nature, terrorism, financial fraud or other problems – that can dramatically impact your enterprise's ability to achieve its objectives. They can damage reputation, market capitalization or other key aspects of your business."
>
> "To succeed today, you must carefully expose your business to increasing levels of risk, monitoring and managing risk as never before."[3]

---

1 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. Http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

2 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

3 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, Pg. 2, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

Preparation for risk is not possible without a plan in place for risk[4] "Risk is constantly 'clouded', abstracted by time, emerging through chains of mistakes, ignored by the best and brightest and even ignited through well-intended actions and incentives."[5]

The stark reality is that the risk of failure can exceed the value of the project. And, yet oil and gas companies, like service companies, simply cannot be risk averse.

B. "Known unknowns" and "unknown unknowns"

Risk events are either anticipated or unanticipated (sometimes called the "known unknowns" and "unknown unknowns").[6] The prediction of low probability, high impact risk events is problematic.

> "We don't live in the world for which conventional risk-management textbooks prepare us. No forecasting model predicted the impact of the current [2008] economic crisis, and its consequences continue to take establishment economists and business academics by surprise.
>
> **…**
>
> Instead of trying to anticipate low-probability, high-impact events, we should reduce our vulnerability to them. Risk management, we believe, should be about lessening the impact [loss] of what we don't understand-not a futile attempt to development sophisticated techniques and stories that perpetuate our illusions of being able to understand and predict the social and economic environment."[7]
>
> "Risk events are the terrible things that happen to organizations that cause the destruction of value, competitiveness, capital or even injury/loss of life. These events can be large and externally driven, such as an unexpected natural disaster or the malicious sabotage of a product. They can be internally driven through mistakes, misinformation, poor design or inadequate safety systems. Lack of skills, purchasing decisions, operational actions, financial or infrastructure/asset decisions, poorly received or delivered communications, failed product launches or deliberate misbehavior can also lead to major risk events. Few business functions escape exposure to risk."[8]

---

4 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 2, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

5 *Id.* at 13.

6 *Id.* at 11.

7 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

8 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 4, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

> "One key to effective risk management is the ability to distinguish between phenomena that cannot reasonably be foreseen and dangers that are "self-inflicted" because they could be avoided by thorough planning and careful execution.
> …
>
> The truth is that risk is often organizational in its origins, created through poor decision-making, misjudgments in planning assumptions, or human error in operations (such as in monitoring or enforcement activities). Many threats are not unforeseeable, but lie just beyond the edge of current knowledge.[9]
> …
>
> Managing risk involves a judicious mix of preventing the risks that can reasonably be controlled, learning to recognize the ones that can't be prevented, being prepared to react to limit damage, and having the resources to recover from the problems that do occur."[10]

C. Black Swan events

"Black Swan" as a risk term is attributed to Nassim Nicholas Taleb.[11] The metaphor refers to:

> "[l]ow-probability, high-impact events that are almost impossible to forecast – we call them Black Swan events – are increasingly dominating the environment. Because of the internet and globalization, the world has become a complex system, made up of a tangled web of relationships and other interdependent factors. Complexity not only increases the incidence of Black Swan events, but also makes forecasting even ordinary events impossible. All we can predict is that companies that ignore Black Swan events will go under."[12]
>
> "Many of the highest-profile risk events are characterized as "black swan" events: sudden, random disasters beyond the ability to control or predict. Examples include major weather and natural events, such as hurricanes and tsunamis. Events on the order of these may seem too big and impractical for an organization or enterprise to manage. But, while the event itself may be beyond

9 Jennings, Will, *The Olympics as a Story of Risk Management*, Harvard Business Review. 13 Aug. 2012. http:/blogs.hbr.org/cs/2012/08/the_olympics_as_a_story_of_ris.html 13 Aug. 2012.

10 *Id*.

11 Taleb Nassim, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, Random House 2001.

12 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

> control, how the crisis is handled – often the biggest threat of organizational damage – is not. And except for completely unpredictable natural disasters, most so-called "black swan" events can be anticipated ahead of time with reasonable foresight and planning."[13]

D. Risk potentation

Complexity and the long time horizon often necessary for completion of a complex undertaking are among the factors which can synergistically potentiate risk.

> "Long timelines mean greater vulnerability to emerging risks - that is, dangers with a large potential impact that are not well understood or easily quantified, or which emerge as the unanticipated result of disparate casual processes interacting."[14]

E. Actual and perceived risk

In the energy business (as in others) "perceived" risk drives public opinion and government regulation. Effective ERM is, in a sense, consistent with *prudent* governmental regulation. The sweet spot for risk appreciation is where actual risk and perceived risk substantially overlap. In communicating with the public and the regulators, energy companies need to address both actual and perceived risks.

F. Loss

Management of risk is intended to prevent the occurrence of loss, and to ameliorate the consequences of loss. [15]

> '"Loss' is a distinct concept [from risk] in that loss requires there to have been an adverse event and for there to have been some consequence as a result of that event. Loss, which can be either partial or total, is, in short, injury or damage sustained by the [company]."[16]

Loss can mean more than direct economic loss. The frictions – *e.g.,* the diversion and distraction of executive and operational attention – associated with a significant loss event can themselves represent a substantial loss to the enterprise.

> "Companies must also expand the traditional view of risk as direct loss to form the broader notion that a missed opportunity or

---

13 Jennings, Will, *The Olympics as a Story of Risk Management*, Harvard Business Review. 13 Aug. 2012. http:/blogs.hbr.org/cs/2012/08/the_olympics_as_a_story_of_ris.html 13 Aug. 2012.

14 *Id*.

15 Pollock, Jeffery, *Risk Management for Black Swan Events: Planning for Nuclear Catastrophe, Fracking Problems and Other Environmental Disasters*, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, at page 6, American Bar Association.

16 *Id*. at 19.

damage to reputation may be as important as a direct loss."[17]

> "Although their impact is the same in economic terms–a dollar not lost, is a dollar earned–risk managers don't treat them equally. They place a greater emphasis on earning profits than they do on avoiding losses. However, a company can be successful by preventing losses while its rivals go bust–and it can then take market share from them."[18]

With Black Swan events, decision-tree economic calculations of the cost of a loss are not particularly helpful; and, in fact, can be counter-productive.

> "In addition, many risk analyses calculate the impact of risk in a way that may drive organizations to deliberately not see such big or "black swan" events. Many organizations simply calculate the cost (*i.e.*, impact) of the risk event and multiply that by the likelihood of it happening. For example, if a risk event is estimated to have an impact of $10,000,000 but is only 1 percent likely to occur, many risk analysts would record an expected loss of $100,000, an amount that may be manageable and acceptable without further action. But, in reality, the impact of the risk event will be either $0 or $10,000,000; therefore the organization must decide if a loss of $10,000,000 is acceptable, a vastly different question from assessing an expected loss of only $100,000."[19]

The cost of an ERM program should not be a deterrent to its implementation. EMR should not be viewed as an optional capability. Nor is ERM accomplished merely by appointing an ERM representative.

> "The cost of an ERM program pales in comparison to the potential massive losses from large risk events. The cost of preparing for an event is usually both small in relative terms and readily incorporated into period budgets and business plans. The cost of non-preparation can be so large as to cause organizational failure. Knowing the scope and value of ERM and, ultimately, doing it at the right time, may make the difference between prosperity and survival versus emergency and disaster."[20]

---

17 Deloitte & Touche, LLP, *Risk Intelligence Series Issue No. 3, The Risk Intelligent Enterprise – ERM for the Energy Industry*, Pg. 7, 13 Jan. 2010. http://www.deloitte.com/view/en_US/us/Services. 17 Aug. 2012.

18 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

19 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 6, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

20 *Id*. at 5.

G. Opportunities

An opportunity can be considered an "upside" risk, with the potential to enhance enterprise value.

> "Events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities."[21]

> "Business leaders who understand their organization's risk are better able to leverage it to create opportunity and competitive advantage."[22]

An effective ERM approach will identify opportunities and will make the appropriate business units aware of the opportunities.

H. The enterprise's risk-bearing capacity

An ERM inquiry is not what risk the enterprise *wants* to bear; rather, what risk is it *able* to bear. For example, what trauma to its earnings per share can the entity sustain and survive? What are the company's risk profile and risk appetite? What is its commitment to risk avoidance and risk response?

Risk education of the company's various units is important. One example is a company's decision to purchase, or not to purchase, certain insurance coverage and certain dollar limits of coverage. The ERM team can be expected to meet with each business unit to explain the insurance coverage, and its absence, in order to impress on the business unit that an uninsured loss will directly impact that unit's balance sheet.

> "[H]aving a clear understanding of the organization's key risks is vital to enable risk activities to be prioritized, monitored and managed. In addition, the risk appetite of the organization needs to be defined, agreed upon and communicated so that risks are being fully considered. Without this knowledge, it is impossible to know whether resources have been correctly allocated, and whether risks are aligned with the organization's strategy.

---

21 Richard M. Steinberg, Miles E. A. Everson, Frank J. Martens and Lucy E. Nottingham, *Enterprise Risk Management – Integrated Framework*, Pg. 2, Executive Summary Committee of Sponsoring Organizations of the Treadway Commission, September 2004.

22 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, Pg. 2, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

> [C]ore elements of the risk process … should be integrated within other key business processes, such as strategic and financial planning, internal audit and procurement. In this way, risk data is considered in the decision making process and the organization is more likely to take appropriate risks within its risk appetite."[23]

I. Severity vs. frequency

Anticipated frequency events pose little threat to the enterprise. In contrast, a Black Swan severe, catastrophic event can cause an immediate demand for cash and other resources of the business.

> "Some risks, especially frequent ones, can be measured in hard numbers (e.g., every week, every quarter), and can have formal risk management programs assigned to them." [24]

> "In areas where risk is relatively routine, such as consumer defaults on payments or credit card fraud, the risk programs become business-as-usual functions and likely not thought of as ERM."[25]

J. Who owns the risk?

Risk remains with the business' operating units. However robust may be a company's ERM capability, ERM remains a process, a facilitator. ERM does not serve to transfer to the ERM process those risks confronting the operating units. And various risk transfer strategies – *e.g.*, insurance and indemnity – cannot be relied upon as a means of transferring all risk. Risk must be understood to remain with the enterprise.

> "While the senior risk executive of the organization, whether or not titled as the Chief Risk Officer, may own and drive the process, the risks themselves are owned by the business units."[26]

III. TRADITIONAL RISK MANAGEMENT

- "Traditionally, risk management fell within corporate accounting or financial departments and only indirectly required input from corporate counsel." [27]

---

23 *Id*. at 8.

24 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 6, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

25 *Id.*

26 *Id.* at 12.

27 Pollock, Jeffery, *Risk Management for Black Swan Events: Planning for Nuclear Catastrophe, Fracking Problems and Other Environmental Disasters*, Pg. 17, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, , American Bar Association.

- "The days of relegating risk management to an outside broker or to the financial department are numbered as today's risk management involves complex legal concepts, cuts across corporate departments, …."[28]
- "Traditional risk management tools are adequate for routine risks such as labor, fire, fleet coverage (auto), and flooding." [29]
- "Because these risks are widespread and numerous, insurance brokers and insurers are able to capably predict what coverage will be appropriate given the risk. Black swan events are different."[30]
- "In most companies, this function historically has been largely the domain of the CFO and finance – based on the notion that most risk is financial and can be mitigated through controls." [31]
- "In certain industries, such as banking, financial markets and insurance, trading risk is the actual business, so the enterprise is focused on creating, selling, managing and servicing risk." [32]
- But even in these companies, many lack a full appreciation for the broader scope of ERM that extends beyond their functional domain or the business they are in."[33]
- "Prior to ERM, traditional risk management addressed risk in organizational silos (e.g. health and safety, insurance, internal audit) from a threat perspective." [34]
- "Driven primarily by increasing regulations and compliance requirements, additional functions, departments and business areas were created to manage the risks associated with compliance obligations."[35]
- "With this increase in risk oversight came fragmented risk and control activities, resulting in increased demands on the business, and "risk fatigue" as business units were asked for the same or similar information from different departments for different purposes."[36]
- "Understanding and defining a clear organization wide risk picture became close to impossible, with duplication of effort and potential gaps in risk coverage. The resulting struggle of executives and boards to determine the adequacy of risk and control efforts led to the birth of ERM."[37]

IV. ENTERPRISE RISK MANAGEMENT("ERM")

A. ERM

ERM is qualitatively distinct from traditional risk management.

---

28 *Id*.
29 *Id.*
30 *Id.*
31 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 2, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).
32 *Id*.
33 *Id*.
34 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 3, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.
35 *Id.*
36 *Id.*
37 *Id.*

i. A scalable, holistic approach

- "Enterprise Risk Management … is a scalable, holistic approach to risk management that combines risk information from across the organization and uses this to meet business objectives and drive business performance and growth by embedding risk management in business processes." [38]

"Scalable," meaning adaptable to increasing demands. "Holistic," meaning focused on the whole and the interdependence of its parts, any one of which can influence another and not necessarily in a linear fashion.

- "In addition to focusing on process, ERM also takes account of the risk culture of the organization, or the behaviors, beliefs and values needed to underpin the actions required by the risk processes."[39]
- "ERM does not take a siloed view of risk, but addresses all types of risk, and can be seen as the sum of Operational Risk, Project Risk, Governance & Compliance, Strategic Risk, Financial Risk and Opportunity Management. Importantly, ERM does not focus only on negative threats, but places as much importance on the exploitation and management of opportunities, or upside risk."[40]

ii. ERM and uncertainty

- "The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders."[41]
- "All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value."[42]
- "Uncertainty presents both risk and opportunity, with the potential to erode or enhance value."[43]
- "Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value."[44]
- "Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."[45]

---

38 *Id*. at 2.
39 *Id.*
40 *Id.*
41 Richard M. Steinberg, Miles E. A. Everson, Frank J. Martens and Lucy E. Nottingham, *Enterprise Risk Management – Integrated Framework*, Pg. 1, Executive Summary Committee of Sponsoring Organizations of the Treadway Commission, September 2004.
42 *Id.*
43 *Id.*
44 *Id.*
45 *Id.*

iii. ERM as a process

- "Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows: Enterprise risk management is:
  - A process, ongoing and flowing through an entity
  - Effected by people at every level of an organization
  - Applied in strategy setting
  - Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
  - Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
  - Able to provide reasonable assurance to an entity's management and board of directors
  - Geared to achievement of objectives in one or more separate but overlapping categories."[46]
- "This definition is … captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors."[47]
- "It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness."[48]

iv. ERM's objectives

- "Enterprise risk management encompasses: [49]
  - **Aligning risk appetite and strategy** – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
  - **Enhancing risk response decisions** – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
  - **Reducing operational surprises and losses** – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
  - **Identifying and managing multiple and cross-enterprise risks** – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
  - **Seizing opportunities** – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
  - **Improving deployment of capital** – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation."[50]

46 *Id.*
47 *Id.*
48 *Id.*
49 *Id.*

- "Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise."[51]
- "This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:
  - **Strategic** – high-level goals, aligned with and supporting its mission
  - **Operations** – effective and efficient use of its resources
  - **Reporting** – reliability of reporting
  - **Compliance** – compliance with applicable laws and regulations."[52]
- "This categorization of entity objectives allows a focus on separate aspects of enterprise risk management."[53]
- "These distinct but overlapping categories – a particular objective can fall into more than one category – address different entity needs and may be the direct responsibility of different executives."[54]
- "This categorization also allows distinctions between what can be expected from each category of objectives."[55]
- "Another category, safeguarding of resources, used by some entities, also is described."[56]
- "Because objectives relating to reliability of reporting and compliance with laws and regulations are within the entity's control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives." [57]
- "Achievement of strategic objectives and operations objectives, however, is subject to external events not always within the entity's control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives."[58]

v. Components of ERM

According to COSO,[59]

> "Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

---

50 *Id.*
51 *Id. at 3*.
52 *Id.*
53 *Id.*
54 *Id.*
55 *Id.* at 2 - 3.
56 *Id.*
57 *Id.*
58 *Id.* at 3.
59 Committee of Sponsoring Organizations of Treadway Commission.

- **Internal Environment** – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting** – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- **Event Identification** – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- **Risk Assessment** – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control Activities** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and Communication** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- **Monitoring** – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.[60]

B. ERM is a risk financing function whose goal is balance sheet protection

Risk financing is intended to provide money to pay for unexpected losses. ERM contributes to that function. The principal reason for ERM is balance sheet protection.

The payment of an insurance premium represents one kind of risk financing function, the financing of the shift to the carrier of the insured risks. Similarly, a company's decision to forego a traditional insurance program in favor of a "captive" program is a risk financing function. Risk financing can include loss portfolio transfers, use of Special Purpose Vehicles, and use of catastrophe bonds ("CAT Bonds") as a few of many examples.[61]

60 Richard M. Steinberg, Miles E. A. Everson, Frank J. Martens and Lucy E. Nottingham, *Enterprise Risk Management – Integrated Framework*, Pgs. 3 and 4, Executive Summary Committee of Sponsoring Organizations of the Treadway Commission, September 2004.

61 *See* Institute of Risk Management, *Study Guide 2007/08: Module Four IRM Diploma in Risk Management*, 2007. *See generally*, Lawrence A. Cunningham, *Securitizing Audit Failure Risk: An Alternative to Damages Caps*, William & Mary Law Review (2007).

C. A few areas of ERM'S application

An ERM practice can influence:

- Enterprise survival at risk
- Cash at risk
- Earnings at risk
- Financial risk
- Currency and interest rate risk
- Reputation and brand risk
- Human error/human risk
- Environmental risk
- Societal risk
- Supply chain disruption[62]
- Raw materials/commodity costs
- Intellectual property risk
- Legal, litigation and compliance risks
- Insurance and indemnity risks
- Operational risks
- Failure of processes and systems
- Strategic risks
- Trading and hedging risks
- Criminal/civil unrest risks
- Terrorism and war risks
- IT attacks
- Geopolitical risks
- Risks in emerging markets
- Natural disasters
- The federal and state statutory and regulatory apparatus, for example,
- Sarbanes-Oxley Act[63]
- Dodd-Frank Act[64]
- Foreign Corrupt Practices Act[65]
- False Claim Act[66]
- Directors and officers liability risks
- Social networking

62 Daniel Gerber and Brian Biggie, *The Global Supply Chain: Understanding, Measuring, Mitigating and Managing Exposure in a Supply Chain Dependent Globalized Market*, Defense Counsel Journal, p. 411, October 2012.

63 15 U.S.C. § 7201, *et seq.*

64 12 U.S.C. § 5361, *et seq.*

65 15 U.S.C. § 78dd-1, *et seq.*

66 31 U.S.C. § 3729, *et seq.* *See* Section X below for further discussion.

V. CAUSES OF RISK OCCURRENCE AND LOSS

Commentators have articulated the causes of risk occurrence and loss[67] in varying but generally consistent ways.

A. "Gambler's Fallacy"

> "As a species we routinely underestimate risk. … One theory behind our persistent failure to adequately perceive risk is the "gambler's fallacy." The gambler's fallacy shows that people have a very poor concept of randomness and assume that if a bad flood occurred in one year, than it is all the more likely that such a bad flood will not occur the following year. (Presumably, the argument would be that the bad event, which is unlikely, has already occurred and therefore will not likely occur immediately again.)"[68]

B. Inability to predict risk[69]

A commentator opines that the inability to predict risk is premised upon a combination of:

- Overconfidence
- Excess optimism
- The "halo effect" (namely that we don't believe bad things will happen to good people, that likeable people are better employees, etc.)
- Anchoring (that previous experience is a solid basis for future predictions)
- Motivational bias (we tend to believe that which is consistent with what will help us)
- Base-rate bias (we tend to ignore factors inconsistent with what we think the answer should be)
- Small-sample/inexperience bias (we are worst at predicting when experience is low)

> "Corporate culture typically requires an optimistic view regarding the legitimacy of leadership and of the business model; hence there is a built-in bias against identifying risk because that risk's presence indicates a potential failure or weakness in the

67 In a legal malpractice setting, representation of "unworthy" clients is a major cause of lawyer liability. *Recent Trends in Lawyers Liability. An examination of the Significant Claims in Fiscal 2011*, Loss Prevention Journal, Volume XXIII, Number 2, Summer 2012 at page 11, Attorneys' Liability Assurance Society, Inc.

68 Pollock, Jeffery, *Risk Management for Black Swan Events: Planning for Nuclear Catastrophe, Fracking Problems and Other Environmental Disasters*, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, at page 17-18, American Bar Association.

69 *Id.* at 18.

corporation. Our ability to anticipate collateral risks is even poorer than our ability to calculate risk."[70]

C. "Institutional Barriers to Effective Risk Prevention"[71]

The discussion and concepts in this section principally derive from the referenced article:

i. Failure to perceive risk[72]

- "Catastrophes are rare and thus often outside of people's experience."
- Causes of failure are multifarious and can include multiple failures.
- Cascading failures can span more than one area of technical expertise.
- Separation of risk assessment personnel and operational personnel.
- Lack of training and understanding or risk management systems.
- Focus on the short term.
- "Normalization of Deviance."
- "Accepting the unusual as normal."
- Reliance on old habits that have worked in the past.
- "It won't happen to us."
    - Rarity of catastrophes
- "Silos"
    - Narrow focus
    - Unawareness of "ripple effect of decisions"
    - Diffused responsibility for issues crossing institutional borders.

ii. "Production Pressure"[73]

- Prevention of risk can retard completion of the project.
- Failure to meet target deadlines
- Prevention increases costs
- Difficulty in measuring the "benefit of preventive action, largely because 'it is only when these measures fail that tracking is possible.'"

iii. Leadership failure[74]

- A lack of "sincere support" of risk prevention by the organization's leadership
- Lack of "buy-in" of risk prevention by senior management
- Management which itself lacks operational or technical expertise
- Discouragement of candid exchange
- A lack of policies and procedures

---

70 *Id.*

71 Kleffner and Campbell, *The Organizational Barriers to Preventing Catastrophes*, Volume 59, Issue 5, Risk Management, 2012 WLNR 13493441; http://www.rmmagazine.com/2012/05/30/the-organizational-barriers-to-preventing-catastrophes/, (2012).

72 *Id.*

73 *Id.*

74 *Id.*

- A lack of accountability and coordination
- When multiple companies are working jointly, inadequate contractual definition of duties

iv. Culture[75]

- Organizational culture
- Team culture
- Impaired candid communication
- "Selective listening" by leadership
- Dilatory communication about perceived risks
- Disrespect and disregard for contrarian opinions
- "Group think"

D. Root cause analysis

A root cause analysis is a "retrospective approach to error analysis – the investigation of the direct or original error that led to an adverse event."[76]

> "A root cause is the most basic causal factor or factors which, if corrected or removed, will prevent recurrence of a situation," writes John Robert Dew, EdD, in an article published in the proceedings of the 56th Annual Quality Congress in 2002.3.[77]
>
> 'There is honest disagreement as to whether or not an error can be attributed to a single root cause … or whether there will be a cluster of causes,' Dew adds. Dew presents five basic root causes:
>
> 1. Putting budget before quality
> 2. Putting schedules before quality
> 3. Putting politics before quality
> 4. Arrogance
> 5. Lack of understanding of knowledge, research, and education."[78]

E. "The Six Mistakes Executives Make in Risk Management"[79]

The authors of this article identify six executive mistakes which, if avoided, can constructively "change the way we think about risk. …" The authors make these points:

---

75 *Id.*

76 *Root Cause Analysis*, Infection Control Today in Articles, Infections, Research & Studies. 7, Nov. 2006. www.infectioncontroltoday.com/articles/2006/11/root-cause-analysis.aspx. 30 July 2012. This article is in a medical context.

77 *Id.*

78 *Id.*

79 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

i. We think we can manage risk by predicting extreme events.[80]

- We have poor record of predicting Black Swan events.
- We become more at risk by focusing on a few extreme possibilities while neglecting other possibilities.
- It is more effective to focus on the consequences---that is, to evaluate the possible impact of extreme events. Realizing this, energy companies have finally shifted from predicting when accidents in nuclear plants might happen to preparing for the eventualities.
- As individuals, we often act "in ways that allow us to absorb the impact of Black Swan events," *e.g.*, by buying insurance.
- Companies must buy insurance to "hedge their risks." Insurance is not [a mere] option.

ii. We are convinced that studying the past will help us manage risk.[81]

- Risk managers mistakenly use hindsight as foresight.
- Hindsight is not foresight. "History fools many."
- Black Swan events do not have precedents.
- Today, "both interdependencies and non-linearities have increased."
- "Some policies have no effect for much of the time and then cause a large reaction."
- Randomness is inherent in socio-economic affairs.
- A tiny number of risky events will cause the majority of losses.
- To "predict both an event and its magnitude … is tough because impacts aren't typical in complex systems."
- There is no such thing as a "typical" failure.

iii. We don't listen to advice about what we shouldn't do.[82]

- "Recommendations of the 'don't' kind are usually more robust than 'do's.'"
- "Although their impact is the same in economic terms–a dollar not lost, is a dollar earned–risk managers don't treat them equally. They place a greater emphasis on earning profits than they do on avoiding losses. However, a company can be successful by preventing losses while its rivals go bust–and it can then take market share from them."
- "The business sections in bookstores are full of success stories; there are far fewer tomes about failure. Such disparagement of negative advice makes companies treat risk management as distinct from profit making and as an afterthought. Instead, corporations should integrate risk-management activities into profit centers and treat them as profit-generating activities, particularly if the companies are susceptible to Black Swan events."

80 *Id.*
81 *Id.*
82 *Id.*

iv. We (mistakenly) assume that risk can be measured by standard deviation.[83]

- "Standard deviation–used extensively in finance as a measure of investment risk–shouldn't be used in risk management."
- "It only means that, in a world of tame [check word] randomness, around two-thirds of changes should fall within certain limits (the -1 and +1 standard deviations) and that variations in excess of seven standard deviations are practically impossible. However, this is inapplicable in real life, where movements can exceed 10, 20 or sometimes even 30 standard deviations. Risk managers should avoid using methods and measures connected to standard deviation, such as regression models, R-squares, and betas."
- "Standard deviation is poorly understood."
- "In any case, anyone looking for a single number to represent risk is inviting disaster."

v. We don't appreciate that what's mathematically equivalent isn't psychologically so.[84]

- "[T]he way a risk is framed influences people's understanding of it. If you tell investors that, on average, they will lose all their money only every 30 years, they are more likely to invest than if you tell them they have a 3.3% chance of losing a certain amount each year."
- "Providing the best-case scenario usually increases the appetite for risk. Always look for the different ways in which risk can be presented to ensure that you aren't being taken in by the framing or the math."

vi. We are taught that efficiency and maximizing shareholder value don't tolerate redundance.[85]

- "Most executives don't realize that optimization [of the enterprise's resources] makes companies vulnerable to changes in the environment."
- "In companies, redundancy consists of apparent inefficiency: idle capacities, unused parts, and money that isn't put to work. The opposite is leverage, which we are taught is good."
- "If you aren't carrying debt on your books, you can cope better with changes."
- "One of the myths about capitalism is that it is about incentives. It is also about disincentives. No one should have a piece of the upside without a share of the downside."
- "Moreover, we shouldn't offer bonuses to those who manage risky establishments such as nuclear plants and banks. The chances are that they will cut corners in order to maximize profits."

---

83 *Id.*
84 *Id.*
85 *Id.*

- "Society gives its greatest risk-management task to the military, but soldiers don't get bonuses."
- "Remember that the biggest risk lies within us: We overestimate our abilities and underestimate what can go wrong. The ancients considered hubris the greatest defect, and the Gods [Nemesis] punished it mercilessly."
- "Any corporation that doesn't recognize its Achilles' heel is fated to die because of it."

F. Human nature[86]

> "What makes risk management so hard? "Risk mitigation is painful; not a natural event for humans to perform."
> …
>
> "JPL engineers graduate from top schools at the top of their class. They are used to being right in their design and engineering decisions. I have to get them comfortable thinking about all the things that can go wrong."
>
> Gentry Lee – Chief Systems Engineer, NASA, JPL[87]

G. Individual and organizational biases inhibit good thinking about risk[88]

The discussion and concepts in this section principally derive from the referenced article. The authors comment:

- We are overconfident about the accuracy of our forecasts
- We anchor our estimates to readily available evidence
- We accept information that supports our initial position, the confirmation bias, and suppress information that contradicts it, cognitive dissonance
- We escalate our commitment to the original course of action, throwing good money after bad, failing to recognize sunk costs
- Group Think: we go along with the flow, suppressing objections to actions that the leader and everyone else seems to endorse.
- We incubate more risk through the normalization of deviance.
- Risk management must overcome these behavioral biases … by deploying active and intrusive processes that:
    - Challenge existing assumptions about the world within and outside the organization
    - Communicate risk information with the use of distinct tools (risk maps, value-at-risk models, stress tests, etc.)

---

86 Robert S. Kaplan, *Risk Management: Interactive Case Study, Jet Propulsion Laboratory*, Pgs. 5 & 6, Baker Foundation, Harvard Business School, http://www.fsmevents.com/palladium/session11/slides.pdf, (accessed July 30, 2013).

87 *Id.*

88 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr 16 Aug. 2012.

- Complement, but do not displace, existing management control practices

H. Mistake chains

> "Many catastrophic risk events are generated within the organization by business decision makers. They are often chains of little mistakes that people either miss, ignore or compound by letting them persist. Then, on top of these, other mistakes are made. Mistake chains happen for many reasons. Sometimes it is a lack of oversight or coordination on the part of different stakeholders or actors within a process. Sometimes perfectly good processes are in place to prevent mistakes, but, for some reason or another, are overridden or ignored. In other cases, an organization's culture may inhibit the questioning of authority or process critique."[89]

Mistake chains often account for airliner crashes.[90]

I. Long time frames

> "Timing, especially long time frames, may be the most confounding and elusive dimension of risk management. Organizations are typically much better at managing recent or frequent risks. Risk events that occur over long time frames, such as five, ten or twenty years, seem to slip from institutional memory quickly after they happen. Those that take decades to manifest are equally difficult to detect and manage."[91]

J. Culture/incentives as a cause[92]

- An organization's culture may also reduce its ability to successfully detect, mitigate and respond to risk.
- The tracking of mistakes or measurement of past decisions may seem to be a waste.
- Many leaders prefer not to spend large amounts of time reviewing their past failures and do not want a continual spotlight on them.
- Others may find risk planning to be hypothetical or theoretical.

---

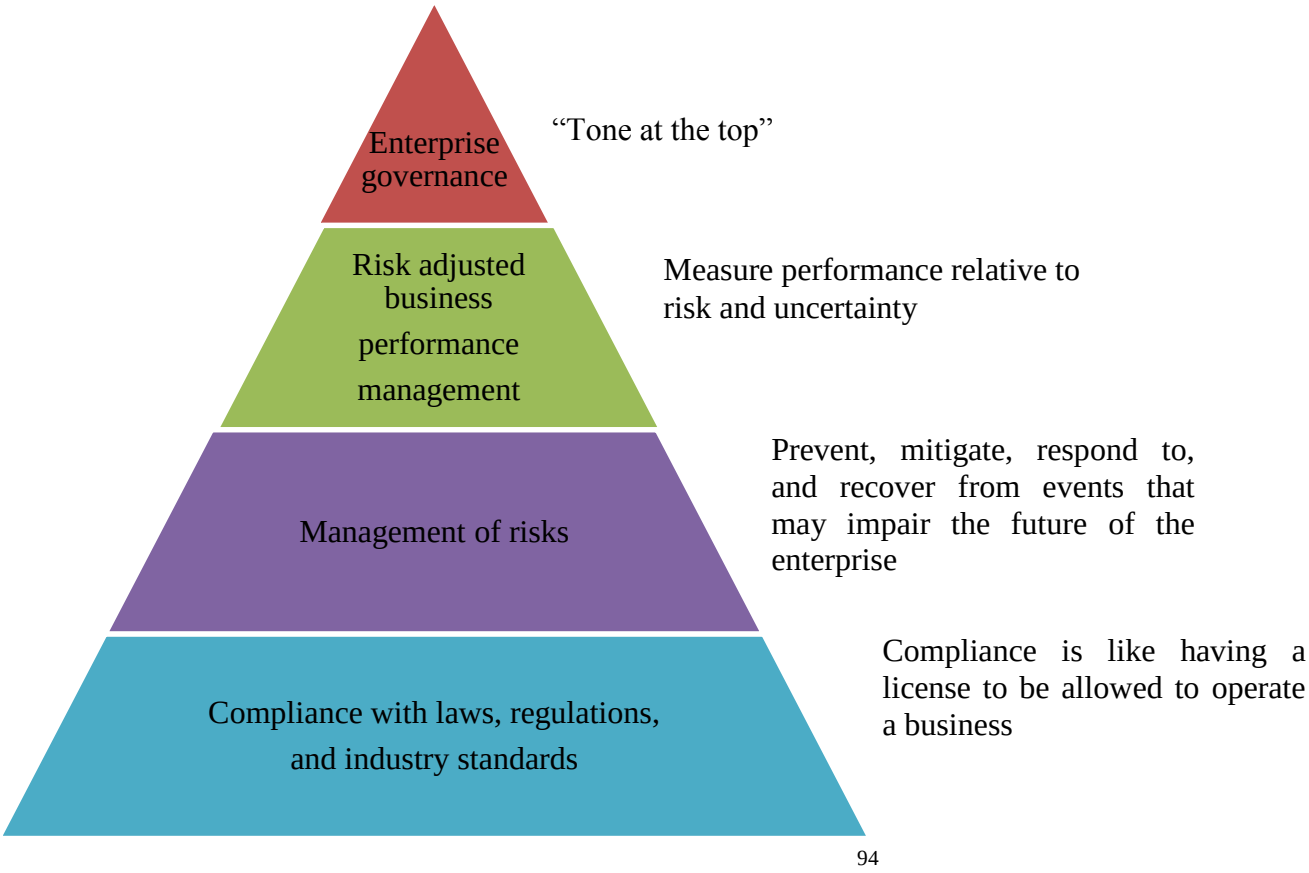
89 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 6, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

90 Patrick Smith, *Asiana Airlines Flight 214: A Pilot's Perspective, Slate On-Line*, http://www.whatispersonalinsurance.com/articles/news_and_politics/transport/2013/07/asiana_airlines.; John Nance, *Comair Crash: When Systems Fail*, August 28, 2006, http://cpf.cleanprint.net/cpf/cpf?action=print&type=filePrint&key=abc_news&url=http%3A%2F%2Fabc...

91 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 7, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

92 *Id.*

- Some may not like the sense of negativity or the focus on failure, instead preferring optimism. With past mistakes out of mind, and future mistakes not thought of, it is all too easy to rely on the optimistic or statistically driven position that "such and such has not happened before or will not happen to us."
- Performance reviews and incentives, such as commission or bonuses, are typically based on short-term performance. As a result, most managers and executives are looking toward the period's performance to gauge their prospects for advancement and reward. This situation is amplified by seniority (in title) as the proportion of total compensation delivered through incentives becomes ever greater. This structure can create cultural environments conducive to seeking super-sized rewards. The tendency in such an environment is to focus on short-term results, not long-term risks.
- During the recent mortgage subprime crisis, one banker remarked: "What's the worst that can happen? We make $200 million and then we get fired."
- As one executive noted, "In a culture of 'got to look good,' there are no risks."
- In most cases, risk events are typically not the result of a single clouding factor, but rather a complex mix of many, making risk management a more complicated enterprise challenge. However, understanding the "clouding" factors of ERM makes their antidotes easier to identify and obtain."[93]



[94]

93 *Id.*
94 *Id.* at 2.

> "Addressing the scope of … [ERM[requires a level of organizational collaboration that culturally and practically can be very difficult to implement. The first step toward creating a robust ERM program encompasses understanding the scope of risk management and nurturing collaboration and preparedness – making it a "team sport" across the enterprise."[95]

K. ERM misfires

A commentator[96] opines that "ERM misfires" are caused by three major factors:

i. Organizations do not know what to do

- The enterprise does not understanding the true scope of risk management.

ii. Clouding factors inhibit successful ERM

- The enterprise is not able to see and/or assess the risks facing it.

iii. Organizations fail to shine the light on the clouding factors and bring the ERM program to life

- The enterprise is unable to undertake key steps that "scatter the clouds."[97]

> "Much of what constitutes poor risk management occurs as a result of misguided or misinformed business decision making. Avoiding mistakes and making good decisions is certainly within the realm of ERM. The first risk management misfire comes when organizations don't understand ERM's scope; they do not know what to do. They feel overwhelmed about risk management – its sheer influence and pervasiveness to the core of nearly every business function, at every moment the business is operating. …
> The question to the decision maker is this: "What position do you want to be in when a risk event happens?" To determine this, organizations and risk managers must first accept that risk events will occur; an organization may avoid them for a period of time, through luck or skill, but at some point negative events will happen."[98]

> "What is hindering their ability to make necessary progress? It comes down to a few simple things: properly defining the scope of ERM, establishing enterprise risk tolerance and driving a culture of sharing risk-related information."[99]

95 *Id.* at 1.
96 *Id.* at 4.
97 *Id.*
98 *Id.* at 5.
99 *Id.* at 1.

> "The challenge for most enterprises is how to implement an ERM program, instill a culture prepared to deal with risk events and learn from inevitable mistakes. Managing enterprise risk is a critical and growing discipline within leading organizations. Doing it right is difficult; many "clouding factors" can sabotage an ERM program at every step. But doing it well may ultimately determine whether your organization can successfully avoid and/or mitigate risks."[100]

Here is another litany of obstacles to effective ERM.

> "**Unrealistic expectations** – ERM is a journey not an overnight solution. Increasing and developing risk management maturity as an organization takes time, effort, money and necessarily involves a significant process of change management, which is not always considered or handled well."[101]

> **"Failure to consider the risk culture** – a successful ERM framework must also consider the behavior, beliefs and values required to support the defined ERM processes. It is unrealistic to expect that all key stakeholders will follow the risk process purely because it has been written down – time and effort has to be invested in communicating the changes, validating understanding and buy-in, and measuring compliance if the framework is to be fully embraced."[102]

> **"Failure to define risk appetite** – "There [is] a failure to properly understand, define, articulate, communicate and monitor risk tolerances, with the mistaken assumption that everyone understands how much risk the organization is willing to take." In most cases, risk appetite and tolerance levels are poorly defined in an organization as those responsible for defining what these boundaries should be, are unable to clearly articulate these levels and gain agreement from all key stakeholders on a value. In particular, placing quantitative rather than qualitative values on these boundaries creates real difficulties, and is quite often placed in the "too hard" bucket. However, without fully defined and communicated risk appetite and tolerance levels, there are no clear guidelines for individuals throughout the organization to understand when they should be exploiting, managing or escalating risks. The end result is that opportunities may be missed, or threats

100 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 1, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

101 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 9, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

102 *Id*. at 9 and 12.

may be accepted that are actually beyond the capacity or willingness of the organization to manage."[103]

"Lack of alignment between risk strategy and business strategy – ensuring that risks are formally considered as part of the strategy definition process means that there is less chance of threats and opportunities being overlooked. Alignment informs the debate as to whether achievement of the organization's strategic aims is, in fact, realistic and can be achieved within the organization's risk appetite. ERM can also be used to drive business performance by embedding risk management within other key business processes, such as financial management, internal audit and procurement, so that there is consideration and informed discussion across all areas of the organization about both the threats and opportunities that need to be managed."[104]

"Poor data management – according to Deloitte, *"[one of] the greatest challenges in implementing an effective ERM program ... [is] integrating data across the organization."* Many organizations struggle with the holistic nature of ERM because they lack the supporting technology to enable data capture, sharing, analysis and presentation on an enterprisewide basis, and in formats suitable for a varying audience. Failure to tell the audience anything they do not already know, or conversely, drowning them with pages of detailed risk information does not encourage participation in, or understanding of, the threats the organization may be facing or opportunities it may be missing."[105]

'"Failure to use enterprise risk management to inform management's decision making for both risk-taking and risk-avoiding decisions.'– despite being a holistic discipline that pulls together risk information from across the organization, risk information is rarely used to inform and drive the decision making process, mainly due to the way the data is accessed and presented to management. Providing the right information to the right people in the right format at the right time is a critical element in proving the value that ERM can bring to the organization."[106]

"Failure to identify executive sponsorship – an executive level sponsor is needed to communicate the importance of the ERM framework at the senior levels of the organization, and to hold peer discussions at the board level. In addition, the sponsor should "act as the face" of ERM to the business, and promote the importance and benefits for the entire organization. Without someone who can

103 *Id.*
104 *Id.*
105 *Id.*
106 *Id.* at 10, 13 and 14.

champion the risk agenda at a senior level, it may be difficult to elevate risk to the board agenda and gain the visibility needed to create action."[107]

"ERM is viewed as synonymous with Governance, Risk and Compliance – another view of ERM is that it is synonymous with GRC (Governance, Risk and Compliance) and is, therefore, overhead intensive. ERM, however, differs from GRC, in that ERM is a driver of strategic value, competitive advantage, and business growth. Unfortunately, due to the corporate and accounting scandals of the late 1990s, "risk management" has become synonymous with Sarbanes-Oxley, which had the unintended consequence of adding tremendous complexity. Rather than adding complexity and "ticking the box" in terms of complying with relevant legislation, ERM is about business performance, profitability and growth; and it is this message that is sometimes misunderstood by key stakeholders."[108]

"The risk management team contains the wrong people – "Senior management should build a risk team with the range of skills needed to meet current business objectives. This blend of skills may need to change over time as the organization becomes more risk mature and starts to roll out an enterprise-wide program." Risk management roles are generally held by individuals with a range of personality types, and these differences, and individual strengths, need to be exploited in the most effective possible manner for the organization. Failure to do so may result in the skill set of the risk team unsuccessfully meeting the needs of the business, particularly as the organization's risk management maturity increases. In addition there is frequently a failure *"...to develop and reward internal risk management competencies"* so that the right behaviors are encouraged or to identify a clear risk career path to encourage individuals to invest their time and effort into the role."[109]

"Failure to identify "quick wins" – the intangible nature of a discipline that deals with uncertainty means that it can sometimes be difficult to quantify the true return on investment of ERM. In addition, the long-term nature of the discipline means that withoutplanning and consideration, it is not always possible to identify "quick wins" and prove the quantified value of ERM. Similarly, unless risk is embedded in business processes such as strategic planning, internal audit, performance management and

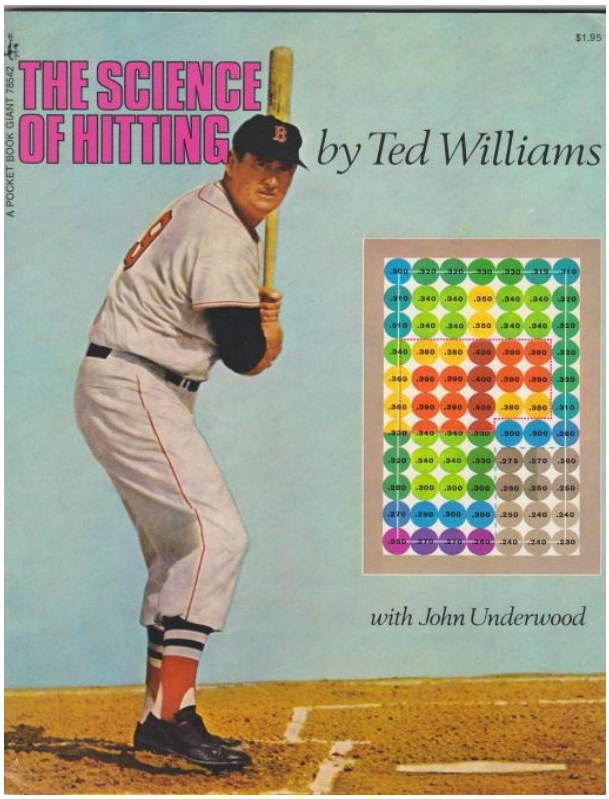
107 *Id*. at 10.
108 *Id.*
109 *Id*. at 10, 15 and 16.

finance, recognizing improvements in business performance and growth cannot definitively be linked to ERM."[110]

VI. EXAMPLES OF ERM

A. Ted Williams

Paul Moomaw of Goshawk Global Investments LLC has written a very insightful article[111] discussing lessons which investors can learn from the art of hitting as practiced by baseball great Ted Williams. Here is a strike-zone grid which appeared on the cover of Williams' book, The Science of Hitting.[112] Moomaw applies the grid in a very interesting way to his investment philosophy. The grid, and Williams' explanation and Moomaw's extrapolation from it, offers insight about ERM.



"Williams devoted himself to knowing his own strike zone. "My strike zone, almost to the inch, was 22 by 32, or 4.8 square feet," writes Williams. Dividing his strike zone into segments the size of a baseball, he calculated that his strike zone was 7 baseballs wide and 11 baseballs high, allowing for pitches on the corners. From practice, experience and knowledge of his own weaknesses, he then applies a precise batting average to each ball in the zone.

110 *Id.*

111 Paul Moomaw, *A Surprise Source of Investment Wisdom: Baseball's Ted Williams*, Goshawk Gloval Investments LLC, July 7, 2011.

112 Ted Williams and John Underwood, *The Science of Hitting*, 1972.

Those are the numbers you see printed on each colored ball. The result is a heat map detailing where Williams had probabilities in his favor—and where he didn't. Example: The deep red circles in the belt-high, middle-plate area are assigned a .400 batting average, because he knew he had great odds when swinging at such pitches."

"My first rule of hitting was to get a good ball to hit. I learned down to percentage points where those good balls were. The box shows my particular preferences, from what I considered my "happy zone"—where I could hit .400 or better—to the low outside corner—where the most I could hope to bat was."

This is the same "know thyself" probabilistic mindset that should be applied to investing.

If you reconstruct the career of Ted Williams by holding his lifetime statistics in one hand and his writings about baseball in the other, **you can only conclude that he was a great goal-setter and a fine risk manager**.

"I think every player should have goals, goals to keep his interest up over the long haul, goals that are realistic and reflect improvement. For me, if I couldn't hit 35 home runs, I was unhappy. If I couldn't drive in 100 runs, if I couldn't hit at least .330, I was unhappy."

Williams took those goals and pieced together a daily strategy for achieving them, a **strategy that included active "risk-management" skills**, to borrow a term from the investment world. If you read what he wrote, it's pretty clear that he had a goal of striking out less than 50 times a year, despite his big swing. (He never struck out more than 50 times in a season past the age of 25.) This is a differentiated strategy for a power hitter. Many power hitters just want to rack up a lot of homers, regardless of how many times they strike out. Williams was different. He thought it was his job to hit home runs *and* to hit for average.

…

In his book, Williams addresses **all manner of risks that must be compensated for**: how to hit with two strikes, how to hit when the wind's blowing in your face, how to adjust to damp and rainy weather. You have to laugh at some examples, but I like the way he tries to think of every risk. He even details a strategy for what to do when you're at bat and a cloud passes overhead and blocks the sun, temporarily decreasing the ambient brightness in the ballpark:

> Unless you know for a fact that your eyes can dilate quickly enough in the split second to adjust to a light that might be half the candle power, you'd be foolish to stand in there and try to hit. Step out and wait until the cloud passes, or until your eyes have dilated and are accustomed to the new light.
>
> This is a man who cared about every at-bat and left little to fate. Like a careful investor who doesn't want to waste money, Williams didn't want to waste at-bats. **He's thinking of risk-management strategies at all times. He's not just crossing his fingers and waiting for the wind to be at his back (baseball's version of a bull market)**.

B. The Olympics

The 2012 London Olympics is an example of an enterprise risk management template.[113]

i. The risks

> "A lot of things didn't happen at the [London] Olympics this year [2012], all of which were extensively prepared for. A terrorist incident, a breakdown of the London rail system, power blackouts, volcanic ash clouds … flooding, an outbreak of infectious disease – the [organizers] spend years thinking about every scenario they could imagine. Simulations of security incidents were rehearsed, and the contingency plans for mass evacuations or emergency situations were put in place."[114]

ii. Complexity, scale and time horizon

> "Risk management is now at the heart of the governance model for the Olympic Games and the Olympic movement and not only because of their growing scale and complexity. There is also the time horizon involved, which can be up to twenty years from the genesis of a host city's bid to the conclusion of the actual event."[115]

iii. Inexperience and noise

> "In planning for the Olympics, warning signals can be imperceptible amidst the noise, due to the relative scarcity of local experience, as organizers tread an unknown path (although there is a growing Olympic professional services complex made up of

113 Jennings, Will, *The Olympics as a Story of Risk Management*, Harvard Business Review. 13 Aug. 2012. http:/blogs.hbr.org/cs/2012/08/the_olympics_as_a_story_of_ris.html 13 Aug. 2012.
114 *Id.*
115 *Id.*

firms and consultants contracted to advise on bid teams and organizing committees)."[116]

iv. Evolution to ERM

"Olympics organizers traditionally focused on reaction and recovery, using tools such as insurance (taken out for personal injury and property coverage), safety plans, and command and control structures. Since the 1980s, however, Games organizing committees have increasingly invested in teams and systems dedicated to the management of risk through internal controls. Risk mitigation is now integrated into decision-making and operations, and no longer treated as just an input into the calculation of insurance premiums."[117]

v. Gaming, stress-testing and scenario planning

"Ensuring readiness for Games-time (in Olympic-speak) now involves strategic pre-emption through stress-testing and scenario planning. Table-top 'gaming' exercises at the top of the chain of command and practical training of personnel through rehearsals are routine across many of the diverse functions of Olympic operations. In the months leading up to London 2012, for example, visible military rehearsals were staged on the River Thames in addition to many test events performed on the main site. Ahead of Vancouver 2010, IT planning identified around six hundred scenarios for rehearsals in a formal playbook which also documented procedures to follow in the event of an incident."[118]

Every Olympic cycle situates the games in a new venue. The Olympics, and other global sports events, have given rise to a new industry: "sports consultants who travel from host city to host city offering experience in various spheres."[119] The International Olympic Committee has a "knowledge management programme [sic] to pass lessons on to the next host."[120]

C. Airline safety

Elsewhere[121] in this paper is a discussion of mistakes chains as often the cause of an airline disaster. Those disasters, however, almost always yield an ERM-type benefit as evidenced by the remarkable passenger survival rate in the July 7, 2013 San Francisco crash on landing of Asiana Flight 214.

116 *Id.*
117 *Id.*
118 *Id.*
119 *The Olympic Legacy, Carrying the Torch*, The Economist, August 18, 2012, page 52.
120 *Id.*
121 *See* Section V(H).

> There is an old saying that FAA regulations "are written in blood." This is a disturbing statement, but true. And because of it, aviation today is an exceptionally safe mode of transportation.
>
> Errors made in aircraft design, production, maintenance, as well as operations by pilots, companies and air traffic control that result in accidents are evaluated by the NTSB, the FAA, and employee unions. The goal of all of these groups is to stop further accident. As noble as that goal is, airplanes will continue to crash.
> ...
>
> The cabin crew of Asiana Flight 214 was able to get all but two out of the aircraft. Had they delayed the evacuation, there likely would have been more deaths and injuries from the fire. The competence of the Asiana cabin crew is in part due to the lessons we have learned from the past.
>
> One of the biggest advances in cabin safety came after an FAA test of what was hoped to be a fire resistant fuel. The test was a complete failure, however the unexpected data from the cabin made major changes to aircraft design and flight attendant training. That data showed the post-impact survivability quickly diminished as the cabin filled with lethal smoke. Changes were made to aircraft interior materials and the focus of rapidly evacuating passengers was incorporated into airline training programs. [122]

VII. ERM'S IMPLEMENTATION

The discussion and concepts in this section principally derive from the referenced article except where otherwise noted.

A. Initiative and authority

- "The success of an ERM capability will ultimately depend on a few critical enablers."
- "The initiative must be championed and supported by people and business units throughout the enterprise."
- "Authority and accountability for risk decision making must be clearly communicated and enforced through an enterprise risk management policy and other guiding documents."
- "… [c]ompanies in the early stages of their ERM journeys might begin by appointing a chief risk officer (CRO) and establishing an enterprise risk management committee."

122 David J. Williams, *Asiana 214: Another Lesson in Aviation safety Coming Right Up*, NYC Aviation Editorial, http://www.nycaviation.com/2013/07/asiana-214-another-lesson-in-aviation-safety-coming - right-up, July 7, 2013.

- "It is crucial to obtain agreement on the sharing of responsibility and accountability for risk management with centralized or corporate areas — such as CRO, legal, regulatory, and insurance, as well as the enterprise risk management committee — and decentralized or business unit areas — such as business unit executives, risk managers, and operating committees."
- "Finally, they should focus on developing basic ERM tools, such as risk registers and reporting dashboards before moving to more advanced tools, such as risk engines and event and loss databases." [123]

B. Priorities

- "Such an approach does not mean that all risk exposures are given equal consideration or are managed in the same way; rather, it means that the enterprise is able to make a more informed and conscious decision on which risks it should actively manage and how it should manage these exposures. For example, the enterprise may elect to self-insure certain nonmaterial exposures depending on its overall risk profile and risk appetite."[124]

C. Data management and technology

- "Data management functionality — the cornerstone of reliable and accurate reporting, valuation, forecasting, and risk measurement — is also under development.
- If the ERM databases are not secure, flexible, and accessible, then the resulting risk analysis, evaluation, and management will be suspect.
- Since a fully functional ERM IT solution for most energy companies will comprise multiple systems and databases, there is little doubt that system and data integration will continue to play a critical role in the success of the overall ERM program."[125]

> "[H]aving consistent risk processes means that risk data escalated within the organization is able to provide a holistic risk picture using comparable terms and figures. Consideration should be given to both internal and external risk reporting, with data tailored for the audience to facilitate ease of understanding.[126]
>
> Ernst & Young believes that *"Effectively harnessing technology to support risk management is the greatest weakness or opportunity for most organizations."* With the ongoing and rapid changes in the external environment, there is an increased need for communication and data sharing across the organization if it is to react quickly and effectively to changing circumstances. As the

123 Deloitte & Touche, LLP, *Risk Intelligence Series Issue No. 3, The Risk Intelligent Enterprise – ERM for the Energy Industry*, Pg. 6, 13 Jan. 2010. http://www.deloitte.com/view/en_US/us/Services. 17 Aug. 2012.
124 *Id*. at 8.
125 *Id.* at 8.
126 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 8, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

Aberdeen Group states: *"The quality of information and data is critically important to effective risk management. However, a common complaint from executives is that the volumes of data and reports produced prevent them from seeing what is truly critical. Highly performing companies have an information technology platform capable of efficiently capturing, processing, and reporting all relevant information."*[127]

Examples of the types of elements to consider for an ERM system include:

- Data repositories
- Early warning systems
- Analytical and modeling tools
- Interdependency frameworks
- Holistic risk connection and consolidation reporting
- BI & integration with other systems"[128]

"Modern ERM software will allow you to implement robust risk tracking and measurement, while providing visibility and transparency to risk data. The very best solutions: deliver a single automated solution to save time and ensure accuracy of data; support homogeneous risk management processes to promote a single risk language across the business; provide checklists, templates and easy access to historical data; facilitate consistent risk reporting; are easily integrated with other internal systems and provide clear audit trails, metrics and key performance indicators to increase overall business effectiveness."[129]

D. ERM recognized as a distinct responsibility

- "Ultimately, ERM must take the form of a combination of capability, process and discipline, each with its own set of techniques, experts, programs and practices supported and invested in across the enterprise." [130]
- "[ERM] must be formally recognized as a distinct responsibility, with pervasive influence across the enterprise and virtually embedded in every decision-making moment."[131]
- "With the inevitability of risk events, an ERM program cannot be founded solely on risk avoidance, but also on preparation for and management of events when they happen."[132]

127 *Id*. at 10.
128 *Id*. at 8.
129 *Id*. at 2.
130 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 8, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).
131 *Id*. at 7.

E. Managing inevitable risk events

- "Much effort is expended on risk prevention activities and not enough on managing inevitable risk events, building response, resiliency, learning and feedback mechanisms.
- Most risk management programs only focus on activities to mitigate or prevent risk."[133]

F. Culture as an essential ingredient to success

- Successful ERM … programs need to become formal responsibilities within the enterprise.
- The ERM function will require authority to establish risk tolerance, implement prevention, mitigation and recovery practices, perform reviews, provide guidance and issue corporate policy.
- It will rarely be a complete clearinghouse or authority on all business decision making, but instead will provide guidance, tools and practices on how decisions should be made.
- In this respect, it should be seen as more a center of excellence than a ruling body or service bureau for vetting business decisions.

If the ERM framework does not take account of the behaviors, beliefs and values that make up the culture needed to support the risk process, there is a strong possibility that the framework will fail. … *"Setting the right risk culture and aligning strategy to risk imperatives are* ***essential*** [emphasis added] *to success in today's new risk era."* "The key to successful enterprise risk management practices depends on the behavioral attributes of the organization at all levels."[134]

G. Incentive compensation[135]

"To create success however, one final step is required, and that is to align incentive compensation with the risks taken by the organization. Specifically, the organization must make sure that short-term results do not generate performance incentives until it is clear that those actions do not degrade its long-term success – in other words, accountability over a longer period of time."[136]

---

132 *Id*. at 8.
133 *Id*. at 8.
134 www.activerisk.com, Active Risk Enterprise Risk Management Readiness Guide, pg. 8, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.
135 *Id*. at 12.
136 *Id*. at 12.

> [T]o emphasize the importance of ERM initiatives and drive home the message regarding expected risk behaviors, the organization may consider implementing a system of sanctions and rewards. For example, personal KPIs (Key performance indicators) may be developed regarding risk activities, such as the timely management of risks, and linked to remuneration to encourage certain behavior. Alternatively, approaches such as "name and shame" may be deployed if certain parts of the business are not acting in accordance with expectations. By shaping behavior, rewards and sanctions are another means to influence the ERM culture, and to demonstrate the commitment of senior management to the importance of ERM."[137]

Monetary incentives to employees for good risk management practices may perversely result in counter-productive, indeed damaging conduct. The argument is that an employee's personal financial gain may motivate the employee to suppress or conceal meaningful risk information.

H. Risk Governance

> "Risk governance helps ensure the correct flow of risk information around the business – to the right people at the right time in the right format – and ensures that risk information supports the decision making process at strategic levels. Key features to consider when defining risk governance procedures include: [138]
>
> **Tone from the top** – the board and executives need to support the ERM framework, and talk and act in a way that promotes the consideration of risk in all business activity.
>
> **Strategies and objectives** – a clear strategy for the ERM framework needs to be articulated, whether purely to meet compliance requirements, and/or to recognize competitive advantage and exploit opportunities. This must be agreed to and understood by the board in conjunction with its risk appetite.
>
> **Alignment to business objectives** – core risk activity should be focused around managing the risks that may have an impact on organizational objectives. As such, there is a need to embed risk management within the strategy-setting process so that it can be used as a driver of business performance.
>
> **Organizational structure** – the accountability and responsibility for ERM needs to be clearly defined across the organization,

137 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 9, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

138 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 7, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.

including establishing clear charters and mandates for the board and its committees that address ERM. In some instances, it may be beneficial for the organization to consider the appointment of a Chief Risk Officer (CRO) or equivalent, who can act as the key ERM sponsor and drive risk activity throughout the business.

Reporting – risk reporting requirements need to be defined and reports tailored depending on the audience. This may vary from high-level dashboard style outputs, to detailed risk register reports. Frequency and ease of understanding should also be considered.

People …Without the right people in the risk team and in key risk positions, whose skills and experience align with the objectives of the ERM initiatives, embedding ERM within the business is a difficult task. The following considerations are key examples of what should be defined when addressing the people aspect of ERM:[139]

Competence and capabilities – individuals appointed into risk positions or those with significant risk responsibilities should have as a minimum a basic understanding of the key ERM principles and practices the organization has defined. Where this is not the case, tailored education and training should be utilized, and/ or external recruitment considered to fill any skills gaps.

Roles and responsibilities – should be clearly defined and communicated. Measuring and monitoring metrics should also be considered to ensure individual understanding of expectations, and to ensure effectiveness/ value of the roles defined.

Ownership & accountability – should be clearly defined, communicated and understood, including ownership and accountability for components of the ERM process, individual risks, controls, mitigation and contingency actions.

Identification of key business supporters – in addition to specific risk roles, it may be valuable for the organization to develop a risk "champions" network of individuals who sit within the business, but who are able to act as the "go to" person within the function or business unit for risk queries. In this way, limited resources within the central risk function can be subsidized, and there is a direct information flow and feedback channel from the business to the risk team and vice versa.

Alignment and coordination – risk roles should be considered from a holistic process across the organization so that there are no unexpected overlaps and duplications in responsibilities, or gaps in

139 *Id.*

> accountability. This avoids unnecessary inefficiencies, and allows resources to be allocated in the most effective manner.
>
> **Process …** Having ERM processes and procedures defined is a key element of the framework. Many standards and leading practice guides exist to help with the definition of risk process. It is, however, important to remember that the process should be customized to the organizational context, be as simple as possible, and leverage existing processes and practice to make it as familiar as possible to the business"[140]

I. The Board of Directors

i. The Board's endorsement of ERM

Endorsement of ERM by the enterprise's Board of Directors and senior management is important. "From several recent studies, it is clear that risk management has become a team sport, successful only when championed by the Board and [executive suite] of an organization and supported by the entire executive team."[141]

Some commentators have proposed that management of risk be directly overseen by a company's Board of Directors.[142] Such an approach can put the Board and its members directly in the litigation mix[143] in the event, for example, of a Black Swan catastrophic event.

> "A question to consider is whether the risk committee is responsible for overseeing the risk management infrastructure — the people, processes, and resources of the risk management program — or whether the audit committee or entire board will oversee it. A related issue is whether the CRO [Chief Risk Officer], if there is one, will report to the risk committee, the board, or the chief executive officer (CEO) — or have a dual reporting relationship to the risk committee, or board, and the CEO.
> …
>
> The board may need to decide whether the risk committee will be responsible for overseeing all risks, or whether other committees, such as the audit committee or the compensation committee, will be responsible for some."

---

140 *Id.*

141 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pg. 12, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

142 Deloitte & Touche, LLP, *Risk Intelligence Series Issue No. 3, The Risk Intelligent Enterprise – ERM for the Energy Industry*, Pg. 9 and 10, 13 Jan. 2010. http://www.deloitte.com/view/en_US/us/Services. 17 Aug. 2012.

143 *See* Section XI below.

> "Increasingly stakeholders are better informed and more interested in how risks to the organization are being managed, with certain groups being prepared to take action if they feel that risk management is not appropriate …. [144]
>
> Companies are, therefore, exposed to an increasing level of risk, with board attention focused on monitoring and managing risk as never before. Boards are requiring insights on whether investments are properly focused and consistent with industry risk issues, and are looking to the risk teams to answer this question. In addition, many organizations are growing significantly in emerging markets, which furthers their need to invest in risk management and internal control activities. As a result of this focus, boards are particularly interested in the risk/reward trade-off, and are keen to understand the benefits of funding a formal ERM program."[145]

ii. The risk committee charter

> "Often, the board and its risk committee define their roles in risk governance by means of the risk committee charter. The charter is also among the main tools the board has for disclosing its approach to risk oversight. In writing the charter, the board and the risk committee will determine the risk committee's role in risk governance.
> …
>
> As public documents, board committee charters specify the committee's responsibilities and how it carries them out. The risk committee charter discloses the board's involvement in and approach to risk oversight, the committee's relationship to the CRO and to management's risk committee, and other key elements of risk oversight.
>
> As with other board responsibilities, it is important that risk oversight does not become a set-it-and-forget-it proposition. Risks in the economic, competitive, regulatory, legal, and technological environments are dynamic, and risk governance must evolve in response."[146]

iii. Education of the Board

The board's effective oversight of ERM requires that the board "is aware of and concurs

144 www.activerisk.com, *Active Risk Enterprise Risk Management Readiness Guide*, pg. 4, July, 2013, http://www.activerisk.com/wp-content/uploads/Enterprise-Risk-Management-Readiness-Guide1.
145 *Id.*
146 *Id.*

with the entity's risk appetite."[147] "The inherent limitations in ERM prevent the board and management from having absolute assurances to achievement of the entity's objectives.[148]

> "NYSE listing standards require that a listed company's corporate governance guidelines address board education. As a relatively new committee dealing with an area in constant flux, the risk committee should consider how it plans to stay informed about developments in risk management practices."[149]

J. A framework

The discussion and concepts in this section principally derive from the referenced article.[150]

i. Preventable Risks

- Risks arising from within the company that generate no strategic benefits
- Risks from employees' and managers' unauthorized, illegal, unethical, incorrect, or inappropriate actions
- Risks from breakdowns in routine operational processes
- Companies should seek to eliminate these risks
- Active prevention: monitoring operational processes and guiding people's behaviors and decisions toward desired norms.

ii. Voluntary Strategy Risks

- Risks voluntarily accepted by the company in order to generate superior returns from its strategy
- Credit risk assumed by a bank when it lends money
- Risks taken on by companies through their R&D activities
- Risks assumed by companies operating in hazardous environments (mining, refining, chemicals, oil and gas exploration, utilities, …)
- Likelihood of strategy risks cannot be reduced to zero
- Risk management should reduce the probability that the assumed risks materialize and improve the company's ability to contain the risk events should they occur
- Companies good at managing their strategy risks can earn superior returns by taking on riskier projects and strategies

147 Richard M. Steinberg, Miles E. A. Everson, Frank J. Martens and Lucy E. Nottingham, *Enterprise Risk Management – Integrated Framework*, Pg. 6, Executive Summary Committee of Sponsoring Organizations of the Treadway Commission, September 2004.

148 *Id.* at 5.

149 Deloitte & Touche, LLP, *Risk Committee Resource Guide for Boards*, pg. 26, July 2012, http://www.deloitte.com/view/en_US/us/Services/additional-services/governance-risk-compliance, 17 Aug. 2012.

150 Robert S. Kaplan and Anette Mikes, *Managing Risks: A New Framework*, Harvard Business Review, http://hbr.org/2012/06/managing-risks-a-new-framekwro/ar/, June 2012.

- Risk stems largely from seemingly unrelated operational choices across a complex organization that accumulate gradually and can remain hidden for a long time
- A "risk awareness" culture among front-line employees, senior executives, and the Board
- Danger for the embedded risk managers to "go native."

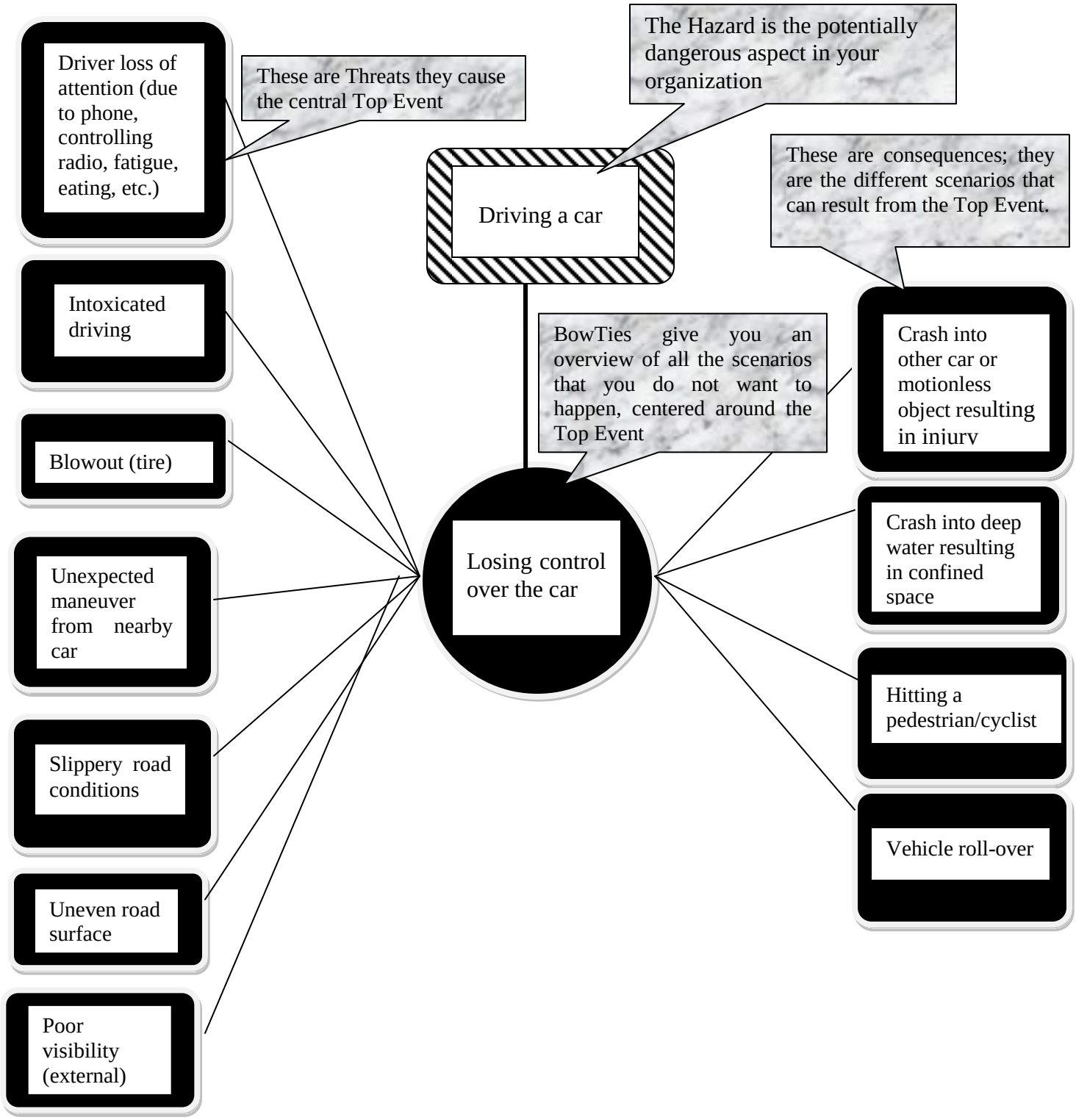
iii. External Risks from Non-Controllable Events

- Natural and geo-political disasters.
- Major macroeconomic shifts.
- Disruptive competitors.
- Management must focus on identification (often such risks are obvious only in hindsight) and mitigation of their impact should they occur.

K. Bowties

ERM "bowties" represent graphic depictions of an ERM template, which can be expanded to deeper levels.[151] See figure below.

151 *See* www.cgerisk.com, CGE Risk Management Solutions, (accessed July, 2013).



L. Risk portfolio framework[152]

The discussion in this section derives from the referenced article.

- IBM … has incorporated a risk portfolio framework for inventorying ERM risk events to support comprehensive analysis.
- The process – usually triggered by the periodic setting of strategic and operational objectives – starts with "identify," a listing and categorization of possible risks that could happen under any reasonable set of circumstances.
- It is important during this step to be expansive and exhaustive in considering different risks: it must extend beyond what happened or what is planned to happen to include what could happen.
- Arguments of authority and emotional critiques should be ignored, and virtually no risk should be ignored as being too unlikely, too preposterous or too devastating.
- The value in this step is in understanding what can or might happen and performing the proper analysis of how to avoid or prevent the potential risk event.
- Even if risk events cannot be avoided or prevented, an organization must understand, prepare and evaluate the consequences of them, including financial or emotional justification (e.g., "failure is not an option").
- An organization needs to take a very broad view of potential risks and build an ERM program with the correct inventory and scope.
- Organizes risks into groups to facilitate appropriate and comprehensive analysis. First, external and internal risk factors are segregated between non-controllable and controllable. With each, risks are categorized for analysis.
- Internal risks, from strategic to operational, are similarly categorized to assess and develop mitigation approaches. For internal risks, fortunately, an enterprise can do much beyond preparation to actually mitigate those risks through controls, business execution and other efforts.
- A risk assessment should take the form of a report or written analysis to assess and plan for the risk. Risks can be assessed for their likelihood, impact and the relative costs to either absorb the risk and/or the costs of investing in ERM (such as assets, safety systems, redundancies, relationships, etc.).
- Risk events that have massive impact should be prioritized highly.
- All risks should be measured on several key dimensions, including likeliness of occurrence, impact if the event occurs (including response and recovery efforts), the cost of preparation/prevention and the velocity or speed at which the risk may emerge.
- This becomes a method of prioritization for planning and the basis for a risk scorecard.[153]

152 Robert Torok, Carl Nordman and Spencer Lin, *Clearing the Clouds: Shining a Light on Successful Enterprise Risk Management*, Pgs. 8 and 9, IBM Global Business Services Executive Report, IBM Institute for Business Value, June 2011, (accessed June, 2013).

153 *Id.* at 9.

M. Risk scorecard and playbook[154]

The discussion in this section derives from the referenced article.

- The risk scorecard may have information such as basic risk information, expected risk, different types of controls, potential impact, opportunity to mitigate, cost of mitigation and recovery requirements.
- The output of this analysis should result in a risk "playbook." Just as a sports team develops a playbook to deal with different contingencies and challenges posed by a defense or offense, the organization should have one to follow in case the risk event seems to be approaching or occurs.
- The playbook will have both specific actions that need to be taken, as well as governing instructions to guide flexible decision making to respond to and mitigate the impacts of the crisis if it occurs differently than expected.[155]

N. Decision controls[156]

The discussion in this section derives from the referenced article.

- A risk monitoring program should be put into place that uses a comprehensive set of key performance indicators (KPIs) or key risk indicators (KRIs) to measure both the impact of risk events and any associated mitigation efforts.
- These are the decision controls used by both management and employees to understand risk events.
- In managing the enterprise "at rest", *i.e.*, during non-crisis times, the steps of monitoring, reporting and reviewing should assess whether chains of mistakes are occurring, and/or whether the likelihood of risk events is changing.
- The objective should be to prevent any events from ballooning into full-blown crises.
- Positive efforts towards breaking mistake chains should be perpetual and persistent, such as a rigorous analysis of causal factors that may influence future risk events.
- The use of data analytics to analyze, measure, model and predict risk is a growing capability among leading enterprises.
- These new tools can add a sophisticated advantage in avoiding, detecting and responding to risk in many categories.

O. Institutional memory[157]

The discussion in this section derives from the referenced article.

- Upon dealing with a risk event (successfully or not), risk managers must be able to look all the way back in the process to the "identify" stage to see how

154 *Id*. at 10.
155 *Id*. at 10.
156 *Id*. at 11.
157 *Id*. at 11 and 12.

accurately they spotted and planned for the particular event, including what the real impact and costs were.

- The knowledge around the risk event must be stored in a formal record of institutional memory and act as an input to review and revise other related risk analyses, playbooks and deployments.
- In risk planning, managers should develop long-term views of the business forward and backward, i.e., extending the time horizon of risk management substantially beyond the immediate future.
- The intent should be to reverse the instinct to only examine recent history and only look into the next period or two.
- When wholly unanticipated risk events occur, the organization should evaluate why it didn't see the event coming and widen its view of risk to be more expansive.
- When anticipated risk events occur, the questions are two-fold: first, did the organization foresee the event with reasonable accuracy; and second, did it reasonably estimate its impact?
- If the answer to either question is negative, the organization needs to treat the event as if it had been an unanticipated event.
- When examining the past, it is more important to examine the validity of the assumptions that were used rather than the decision itself.
- Even the most carefully made decisions can be wrong if their underlying assumptions or facts were incorrect.
- Achieving this will likely require a different approach than merely relying on memories and personal experience.
- An institutional memory must be codified in a formal way in a system, complete with its own formats, procedures, update processes and incentives for use.
- The institutional memory must also forego bias, flattery and revisionist history.
- The bad stuff that happens – despite being painful to examine and remember – is extremely valuable.
- Ultimately, this institutional memory helps create an ERM-enabled enterprise.

VIII. ERM IN THE OIL AND GAS INDUSTRY

According to Deloitte:[158]

A. Traditional risk management

- "Several energy companies have designed and implemented robust risk management capabilities, particularly in traditional areas such as insurable hazard risks related to natural disasters and similar events as well as readily quantifiable financial risks.

158 Deloitte & Touche, LLP, *Risk Committee Resource Guide for Boards*, pg. 26, July 2012, http://www.deloitte.com/view/en_US/us/Services/additional-services/governance-risk-compliance, 17 Aug. 2012. According to this article, The Committee of Chief Risk Officers is developing best practices for ERM for energy companies.

- In a recent survey …, the vast majority of energy companies polled indicated that they are pursuing a formal ERM program while very few indicated that their ERM capabilities were fully operational.
- Many energy companies have developed fairly robust approaches to manage a few risk types in isolation, including insurable hazard risks and readily quantifiable market (or price) risk and credit risk.
- Some also rely on relatively haphazard or unsophisticated quantitative and qualitative risk analysis techniques to address other risk types on an individual basis.
- Many energy companies also focus their risk management activities on business units that are assumed to include the most significant risk exposures such as commodity trading.
- Moving beyond a fragmented ERM capability involves expanding the coverage of risk management activities to encompass all material risk types and business units.

B. Evolving ERM capabilities[159]

- "Many energy companies have experienced difficulty adopting ERM for a variety of reasons, including resistance to perceived centralization of responsibilities, lack of well-defined objectives, fragmented accountability, lack of resources, and inadequate data, systems, and infrastructure.[160]
- For various reasons, the financial services industry and, more recently, the energy industry have become early adopters and pioneers in the ongoing evolution of the ERM capability.

C. International risks[161]

- "Energy companies also face an array of political, legal, and regulatory risks.
- Those with international operations are particularly susceptible to commercial and security threats arising from currency inconvertibility or transfer restrictions, breach of sovereign contracts, nationalization, confiscation or "creeping" expropriation of energy assets, and war and civil unrest.
- Recent events affecting oil and gas companies in Venezuela demonstrate the uncertainty and potential for losses caused by political risk as well as some potential remedies."

D. Operational risks[162]

- "Oil and gas companies continue to struggle with the processes to estimate and disclose reserves while electric utilities and their customers experience outages caused in part by human error and information system failures.

159 *Id.*
160 *Id.*
161 *Id.*
162 *Id.*

- Hurricane Katrina and the August 2003 blackout illustrate the nature of operational risks for energy infrastructure and the potential economic, social, and environmental impacts."

E. Portfolio Effects[163]

- "Once an energy company has expanded coverage across risk types and business units, the next step may be the integration and aggregation of these exposures to provide a truly enterprise perspective.
- Such a perspective is critical for informed "top-down" management of the enterprise's risks, while more detailed attention to each particular risk type or business unit is required for effective "bottom-up" management of specific exposures.
- Adopting a portfolio view of risk allows energy companies to take advantage of naturally offsetting risk exposures and opportunities to optimize risk treatment strategies.
- For example, energy companies might decide to rationalize insurance to cover residual rather than inherent risk exposures or share certain risk exposures through joint ventures with other companies."

IX. MACONDO

Much has been written[164] about the failures leading up to the Macondo well blow out in 2010.

In its Report on Macondo,[165] the National Academy of Sciences made the following Findings, Summary Observations and Summary Recommendations, which reflect the absence of effective cross-disciplinary enterprise risk management during the planning and operational stages. Highlighted in bold are those conclusions which implicate ERM.

A. Summary Findings[166]

1. The flow of hydrocarbons that led to the blowout of the Macondo well began when drilling mud was displaced by seawater during the temporary abandonment process.

2. The decision to proceed to displacement of the drilling mud by sea-water was made despite a failure to demonstrate the

163 *Id*.

164 Suich, Joseph, *Controlling Environmental Risk Before It Enters or Leaves a Company and How Outside Counsel Can Add Value in this Process*, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, pg. 25, American Bar Association. *See also*, *Deepwater Horizon Oil Spill Litigation Database*, Environmental Law Institute, http://www.eli.org/Program_Areas/deepwater_horizon_oil_spill_litigation_database_results.cfm?case_type=Envirnmental. *See, e.g.*, Russell Gold, *Leaking Oil Well Lacked Safeguard Device*, Wall St. J., http://online.wsj.com/article/SB10001424052748704423504575212031417936798.html, Apr. 28, 2010.

165 www.national-academies.org, *Macondo Well-Deepwater Horizon Blowout: Lessons for Offshore Drilling Safety*, National Academy of Science, http://www.nap.edu/catalogue.pho?record_id=13273, (2012).

166 *Id*. at 6.

integrity of the cement job even after multiple negative pressure tests. This was but one of a **series of questionable decisions** in the days preceding the blowout that had the effect of reducing the **margins of safety** and that evidenced a **lack of safety-driven decision making**.

3. The reservoir formation … posed significant challenges to isolation using casing and cement. The approach chosen for well completion **failed to provide adequate margins of safety and led to multiple potential failure mechanisms**.

4. The loss of well control was not noted until more than 50 minutes after hydrocarbon flow from the formation started, and attempts to regain control by using the BOP were unsuccessful. The blind shear ram failed to sever the drill pipe and seal the well properly, and the emergency disconnect system failed to separate the lower marine riser and the Deepwater Horizon from the well.

5. The BOP system was **neither designed nor tested** for the dynamic conditions that most likely existed at the time that attempts were made to recapture well control. Furthermore, the design, test, operation, and maintenance of the BOP system were **not consistent with a high-reliability, fail-safe device**.

6. Once well control was lost, the large quantities of gaseous hydrocarbons released onto the Deepwater Horizon, exacerbated by low wind velocity and **questionable venting selection**, made ignition all but inevitable.

7. The actions, policies, and procedures of the corporations involved **did not provide an effective system safety approach commensurate with the risks** of the Macondo well. **The lack of a strong safety culture** resulting from a deficient overall systems approach to safety is evident in the **multiple flawed decisions** that led to the blowout. **Industrial management** involved with the Macondo well–Deepwater Horizon disaster **failed to appreciate** or **plan for the safety challenges** presented by the Macondo well.

B. Summary Observations[167]

1. …, **alternative completion techniques and operational processes were available that** could have been used to prepare the well safely for temporary abandonment.

2. The ability of the oil and gas industry to perform and maintain an integrated assessment of the margins of safety for a

167 *Id*. at 7.

complex well like Macondo is impacted by the **complex structure of the offshore oil and gas industry and the divisions of technical expertise among the many contractors engaged in the drilling effort.**

3. The **regulatory regime was ineffective in addressing the risks** of the Macondo well. The actions of the regulators **did not display an awareness of the risks** or the very narrow margins of safety.

4. The extent of **training of** key personnel and decision makers both in industry and in regulatory agencies **has been inconsistent with the complexities and risks of deepwater drilling.**

5. Overall, neither the companies involved nor the regulatory community has made effective use of real-time data analysis, information on precursor incidents or near misses, or lessons learned in the Gulf of Mexico and worldwide to adjust practices and standards appropriately.

6. Industry's and government's research and development efforts have been focused disproportionately on exploration, drilling, and production technologies as opposed to safety.

C. Summary Recommendations[168]

1. …, **guidelines should be established** to ensure that the design approach incorporates **protection against the various credible risks** associated with the drilling and completion processes.

2. All primary cemented barriers to flow **should be tested** to verify quality, quantity, and location of cement. The integrity of primary mechanical barriers … **should be verified** by using the best available test procedures. All tests should have **established procedures and predefined criteria** for acceptable performance and should be subject to independent, near-real-time **review** by a competent authority.

3. BOP systems should be redesigned to provide robust and reliable cutting, sealing, and separation capabilities for the drilling environment to which they are being applied and under all **foreseeable operating conditions** of the rig on which they are installed. **Test and maintenance procedures should be established** to ensure operability and reliability appropriate to their

168 *Id.*

environment of application. Furthermore, advances in BOP technology should be evaluated from the **perspective of overall system safety**. Operator training for emergency BOP operation should be improved to the point that the full capabilities of a more reliable BOP can be competently and correctly employed when needed in the future.

4. **Instrumentation and expert system decision aids should be used** to provide timely warning of loss of well control to drillers on the rig (and ideally to onshore drilling monitors as well). If the warning is inhibited or not addressed in an appropriate time interval, **autonomous operation** of the blind shear rams, emergency disconnect system, general alarm, and other **safety systems** on the rig should occur.

5. **Efforts to reduce the probability of future blowouts should be complemented by capabilities of mitigating the consequences** of a loss of well control. Industry should ensure timely access to demonstrate well-capping and containment capabilities.

6. The United States should fully implement a hybrid regulatory system that incorporates a limited number of prescriptive elements into a **proactive, goal-oriented risk management system** for health, safety, and the environment.

7. … regulators should identify and enforce **safety-critical points** during well construction and abandonment that warrant **explicit regulatory review and approval** before operations can proceed.

8. A single U.S. government agency should be designated with responsibility for ensuring an **integrated approach for system safety** for all offshore drilling activities.

9. Operating companies should have ultimate responsibility and accountability for well integrity, because only they are in a position to have **visibility into all its aspects**. **Operating companies should be held responsible and accountable** for well design, well construction, and the suitability of the rig and associated safety equipment. Notwithstanding the above, the **drilling contractor should be held responsible and accountable** for the operation and safety of the offshore equipment.

10. Industry should greatly **expand R&D efforts** focused on improving the overall safety of offshore drilling **in the areas of design, testing, modeling, risk assessment, safety culture, and systems integration**. Such efforts should encompass well design,

drilling and marine equipment, **human factors, and management systems**. These endeavors should be conducted to benefit the efforts of industry and government to instill **a culture of safety**.

11. Industry, BSEE, and other regulators should undertake efforts to expand significantly the **formal education and training** of personnel engaged in offshore drilling to support proper **implementation of system safety**.

12. Industry, BSEE, and other regulators should **improve corporate and industry-wide systems for reporting safety-related incidents**. Reporting should be facilitated by enabling anonymous or "safety privileged" inputs. Corporations should investigate all such reports and disseminate their **lessons-learned findings** in a timely manner to all their operating and decision-making personnel and to the industry as a whole. **A comprehensive lessons-learned repository should be maintained for industry-wide use**. This information can be used for training in accident prevention and continually improving standards.

13. Industry, BSEE, and other regulators should foster an effective safety culture through consistent training, adherence to principles of human factors, system safety, and continued measurement through leading indicators.

X. ENVIRONMENTAL ENTERPRISE RISK MANAGEMENT

Energy and other companies can benefit from the implementation of enterprise risk management in an environmental context. An effective program can have salutary effects in unanticipated ways.

The False Claims Act ("FCA")[169] creates a cause of action against a person who knowingly submits to the federal government a false claim for payment.

> "False representations of compliance with environmental regulations that are incorporated into governmental contracts are considered false claims."[170]

A defense is that the government knew of the false statement, or did not rely on it, or waived the contractual provision.[171] The author opines:

> "An ERMS [environmental enterprise risk management program] that has its results available to the government can be effective in

169 31 U.S.C. § 3729, *et seq.*

170 Linda Guinn, *Environmental Enterprise Risk Management Benefits for a Government Contractor*, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, Pg. 7, American Bar Association.

171 *Id.* at 8.

> proving government knowledge of environmental non-compliances and potential violations."[172]

ERMS reduce FCA risk because the ERMS protocol promotes early identification and resolution of problems; discourages government interest; and provides a robust defense framework.[173]

> "A good ERMS may make a multi-million dollar difference in an FCA case. When discussing an ERMS with Senior Management, the inclusion of the risk from the FCA makes the return on investment calculation for an ERMS highly attractive."[174]

Federal judges use sentencing guidelines in assessing punishment in criminal prosecutions.[175] "Many companies pattern their ERMS on the sentencing guideline requirements in order to more easily promote the organization's [criminal] defense"[176] to an FCA action alleging environmental wrongdoing and to demonstrate the enterprise's due diligence.

XI. LITIGATION IMPLICATIONS OF ERM

The specific litigation-avoidance goals of an enterprise risk management strategy are: (1) to prevent risks and resulting litigation; (2) to implement ERM without inevitable creation of a road map of litigation liability; and (3) to propose ameliorative litigation strategies in anticipation of litigation and formal lawsuit discovery.

A. Litigation anxiety

In the course of planning and preparation to avoid catastrophic mishaps, companies can engage in all manner of prospective risk management and self-evaluation, whether done voluntarily in the exercise of ordinary care, done further to industry standard or done pursuant to governmental mandate.

Effective and meaningful pre-incident assessment of risks needs to be uninhibited and deliberative. In any complex endeavor, matters of judgment are presented. Effective ERM presupposes candid and forthright identification and assessment of risks, and responsive strategies. The prospect of litigation arising from a future event might inhibit candor in some participants to the ERM process. In other participants, the litigation prospect might promote unwarranted and intense attention on the most remote and hypothetical of risks. In either case, the legitimate aims of effective ERM can be thwarted by the litigation overlay.

In one scenario a risk is identified in the planning process. It is evaluated as remote, requiring no curative response. Or perhaps, the measures taken in response to the identified risk prove to be ineffective. Either way, this risk causes a catastrophic event.

---

172 *Id.*
173 *Id.* at 7.
174 *Id.* at 6.
175 USSG, § 8B2.1 (2010).
176 Linda Guinn, *Environmental Enterprise Risk Management Benefits for a Government Contractor*, In-House Counsel Committee Newsletter, Vol. 13, No. 1, May 2012, at page 7, American Bar Association.

Does the identification, assessment and management of risk create a litigation road map? Do the litigation implications chill the risk analysis? How can the utility of the process be promoted in a litigation environment?

B. "Heroes' Risks"

There are personal risks to an individual whose risk management position is too provocative for his organization. The referenced article[177] describes these as "Heroes' Risks" include:

- Career risk
- Professional ostracism
- Loss of status
- Financial loss
- Loss of credibility

C. Hindsight bias vs. "Same or Similar Circumstances"

ERM practice would expect a retrospective, thorough review of a bad risk outcome and whether the risk had been anticipated, etc. Of course, the "retrospectroscope" is flawless. A delimma is that "[m]any threats are not unforeseeable, but lie just beyond the edge of current knowledge."[178]

> "Hindsight bias has pernicious effects on the evaluations of decision makers. It leads observers to assess the quality of a decision not by whether the process was sound but by whether its outcome was good or bad … This outcome bias makes it almost impossible to evaluate a decision properly – in terms of the beliefs that were reasonable when the decision was made … When the outcomes are bad, the clients often blame their agents for not seeing the handwriting on the wall-forgetting that it was written in invisible ink that became legible only afterward. Actions that seemed prudent in foresight can look irresponsibly negligent in hindsight."[179]

Texas law acknowledges, at least to a degree, that a defendant's conduct should not be judged (only) by the outcome. The Texas Supreme Court has promulgated jury questions in negligence cases. Those questions direct the jury to find whether the defendant was "negligent," based on the "same or similar circumstances" existing at the time of the occurrence.

---

177 Taleb, Nassim, Goldstein, Daniel G., and Spitznagel, Mark W., *The Six Mistakes Executives Make in Risk Management*, Harvard Business Review. Oct. 2009. http:/hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management/ar/pr, 16 Aug. 2012.

178 Jennings, Will, *The Olympics as a Story of Risk Management*, Harvard Business Review. 13 Aug. 2012. http:/blogs.hbr.org/cs/2012/08/the_olympics_as_a_story_of_ris.html 13 Aug. 2012.

179 Daniel Kahneman, *Thinking, Fast and Slow*, pp. 203-204 (2011)i; H. S. Grace & Co., Inc., Litigation Trustee Claims Against Directors and Officers in Bankruptcy Proceedings – Examining the External Environment, Defining the Difference #64 (February 2013).

> "'Negligence' means failure to exercise ordinary care, that is, failing to do that which an [oil company] of ordinary prudence would have done under the *same or similar circumstances* or doing that which an [oil company] of ordinary prudence would not have done under the *same or similar circumstances*." [180]

Defense counsel argue that this Court instruction requires that the jury not utilize the "retrospectroscope" to evaluate with hindsight defendant's conduct; rather, the jury is to consider defendant's conduct as it occurred at the time of the event, which represents the "same or similar circumstances."

Litigation-wise, ordinarily a jury is more forgiving and accepting of a defendant [*e.g.*, a defendant energy company], which made an informed judgment on a difficult issue – later proven wrong (*i.e.*, by the occurrence of a subsequent incident) – than of a defendant who failed to consider the issue at all.

D. Privilege of critical self-evaluation

A catastrophic event occurs. There ensues a plethora of investigations of the implicated company, including of course an investigation of the company by the company. The litigation discovery privileges, if any, which might attach to the company's post-incident self-evaluation and self-investigation are familiar, if not necessarily consistent from jurisdiction to jurisdiction. This *retrospective* assessment by the company of its own conduct generates intense legal competition between the company seeking to preserve the confidentiality of its self-examination and plaintiffs' counsel seeking its discovery as a roadmap to civil liability for those damaged by the event.

One privilege often advanced by a defendant company to shield from litigation discovery its retrospective self-analysis is the privilege of critical self-examination or the self-evaluation privilege ("SEP").[181] And this retrospective self-examination is the kind of inquiry which the ERM literature promotes usually, however, without recognition or appreciation of its litigation implications.

What about a company's *prospective* self-assessment, that is, one which occurs prior in time to a catastrophic event and as part of an ERM undertaking? Can the SEP protection from litigation discovery attach to a pre-incident risk analysis? If not, should it? And if not, then what? Plaintiffs' counsel will be no less eager to discover a *prospective* risk analysis than a *retrospective* self-assessment. The privilege from discovery which can sometimes attach to a prospective self-evaluation is not nearly as familiar – or as judicially recognized – as that arising in a retrospective self-analysis post-incident.

An ERM program should take into account the:

- Presumption of litigation discoverability of all pre-incident risk analysis

180 Texas Pattern Jury Charges, "General Negligence," Section 2.1 (2010).

181 The courts are inconsistent and unreliable in their recognition of this privilege.

    - Discovery includes all electronic communications and other materials
- Distinction between prospective and retrospective risk assessment
- Presumption of discovery of pre-incident assessment contradicts policy goal of a robust ERM protocol.
- Potential liability for failure to have competent pre-incident risk assessment
- Foreseeability analysis
    - Is an identified risk in the ERM playbook necessarily a "foreseeable" risk?

E. Ameliorative litigation strategies

- Employee education
    - Thoughtful documentation including electronic documentation
- Indemnity and insurance
    - Contractual transfer of risk
    - Indemnity only as good as the financial wherewithal of the indemnifying party
    - Do not provide 100% protection from all risks
    - Risks remain with the enterprise
- Application of *Daubert* principles to exclude evidence of ERM – enumerated risks which are not scientifically plausible
    - But if the ERM – enumerated risk in fact occurred and is the basis of the litigation, doesn't this satisfy *Daubert*?
- Joint ventures and similar inter-company arrangements