The C-Levels role in managing the organization's enterprise risk management (ERM)

Financial Executives International Annual Conference
Ottawa, June 2011

Garry McDonell
National Director
Aon Global Risk Consulting

AON

Agenda

- Who is in the audience?
- A little revisionist history.
- What our collective clients are saying about ERM.
- The Hallmarks of a Good ERM Program.

TOPIC: Risk Management
Session overview

- Formal Presentation Overview
  - How should the C-levels manage an organization's enterprise risk management and keep the Board fully informed on its practices so that it can exercise its required oversight?
- Informal Presentation Overview
  - How can the C-level manage all the hype around enterprise risk management, effectively manage risk and keep the Board informed so that it can exercise its required oversight?

Our Understanding of What You Do

- It is the responsibility of the financial executive to manage the financial position of the division, support the overall corporate mission and ensure that all tools are utilized to guarantee success.
- At the heart of the organization, the function extends from corporate to divisional and international operations
- Expected to find best practices in a cost efficient package
- Find sources of funding, ways to grow the business, manage cash
- Manage conflicting priorities.
- Communicate internally and externally.
- Operate with utmost discretion when using
- Management of Risk

Is that about right?

An Historical Perspective

- In the past few years marquee companies collapsed, high profile executives stepped down in disgrace and 1,289 financials were restated.
- Risk Management Committees were developed, CEOs hired chief risk officers and organizations spent $6 billion on Sarbanes-Oxley compliance.
- Nassim Nicolas Taleb's The Black Swan is published by Random House in New York. It is a warning that "our world is dominated by the extreme, the unknown, and the very improbable . . . while we spend our time engaged in small talk, focusing on the known and the repeated."

An Historical Perspective

- Thucydides, in the early 400 BC, who proposed a “new penetrating realism,” one that “removed the gods as explanations of the course of events.” Thucydides was “fascinated by the gap between expectation and outcome, intention and event.” Perhaps he should be called the father of risk management.
- 1962 – In Toronto, Douglas Barlow, the insurance risk manager at Massey Ferguson, develops the idea of “cost-of-risk,” comparing the sum of self-funded losses, insurance premiums, loss control costs, and administrative costs to revenues, assets and equity. This moves insurance risk management thinking away from insurance, but it still fails to cover all forms of financial and political risk.

An Historical Perspective

- 1992 – British Petroleum turns conventional insurance risk financing topsy-turvy with its decision, based on an academic study by Neil Doherty of the University of Pennsylvania and Clifford Smith of the University of Rochester, to dispense with any commercial insurance on its operations in excess of $10 million.
- 1992 – The Cadbury Committee issues its report in the United Kingdom, suggesting that governing boards are responsible for setting risk management policy, assuring that the organization understands all its risks, and accepting oversight for the entire process.
- 1993 – The title “Chief Risk Officer” is first used by James Lam, at GE Capital, to describe a function to manage “all aspects of risk,” including risk management, back office operations, and business and financial planning.

An Historical Perspective

- 1995 – A multi-disciplinary task force of Standards Australia and Standards New Zealand publishes the first Risk Management Standard, AS/NZS 4360:1995, bringing together for the first time several of the different sub disciplines.
- That same year Nick Leeson, a trader for Barings Bank, operating in Singapore, finds himself disastrously over-extended and manages to topple the bank. This unfortunate event, a combination of greed, hubris, and inexcusable control failures, receives world headlines and becomes the “poster child” for fresh interest in operational risk management.

An Historical Perspective

- 1996 – Peter Bernstein's Against the Gods: The Remarkable Story of Risk Bernstein's book, while first a history of the development of the idea of risk and its management, is also, and perhaps more importantly, a warning about the over-reliance on quantification.
- 1998 – The collapse of Long-term Capital Management, a four-year-old hedge fund, in Greenwich, Connecticut, and its bailout by the Federal Reserve, illustrate the failure of over-reliance on supposedly sophisticated financial models.
- 2000 – The widely heralded Y2K bug fails to materialize, in large measure because of billions spent to update software systems. It is considered a success for risk management.
- 2001 – The terrorism of September 11 and the collapse of Enron remind the world that nothing is too big for collapse. These catastrophes reinvigorate risk management.

An Historical Perspective

- 2002 – In July, the U. S. Congress passes the Sarbanes-Oxley Act, in response to the Enron collapse and other financial scandals, to apply to all public companies. It is an impetus to combine risk management with governance and regulatory compliance. Opinion is mixed on this change. Some see this combination as a step backwards, emphasizing only the negative side of risk, while others consider it a stimulus for risk management at the board level.
- 2003 – In the face of growing complaints from shareholders in the spring of 2003 company chairman Conrad Black publicly dismissed corporate governance as a “fad.” He described as “zealots” those investors who called for corporate governance principles to be instituted in the company he had founded.
- 2007 – The United States Federal Reserve bailout of Bear Stearns appears to many to be an admission of the failure of conventional risk management in financial institutions.

An Historical Perspective

- 2005 – Bernard Ebbers, former chief executive of WorldCom Inc., convicted of security fraud and conspiracy charges after his firm misstated some $11 billion worth of accounts.
- 2009 – Bernie Madoff pleads guilty to an 11 count criminal complaint, admitting to defrauding thousands of investors. On 29 June 2009 this white-collar criminal was sentenced to 150 years in prison.
- and on it goes…..

Is it all about profit?

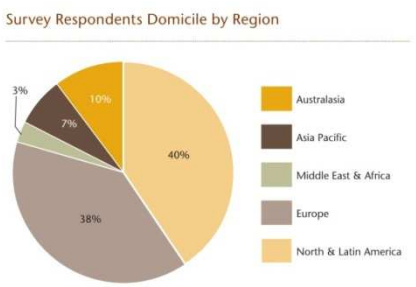
- 2011 The Business Ethics Blog Chris MacDonald, stated
- Despite the fact that the traditional corporate (and anti-corporate) rhetoric has focused on the significance of profits, it's probably much more likely that corporations and the key decision-makers within them are moved by a much broader range of motives, including things like:
  - A desire to increase market share;
  - The desire to innovate;
  - The desire to create cool products;
  - Basic competitive drives to be (and prove yourself to be) bigger, stronger, faster, smarter, etc.;
  - The CEO's desire to build his or her personal legacy;
- Is it "Motivated Blindness"?

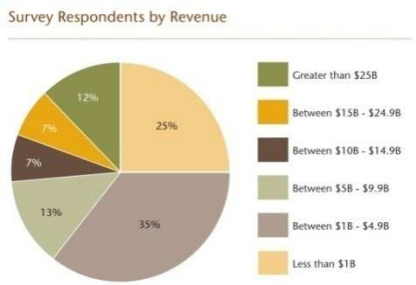
2010 Aon Global ERM Survey Overview

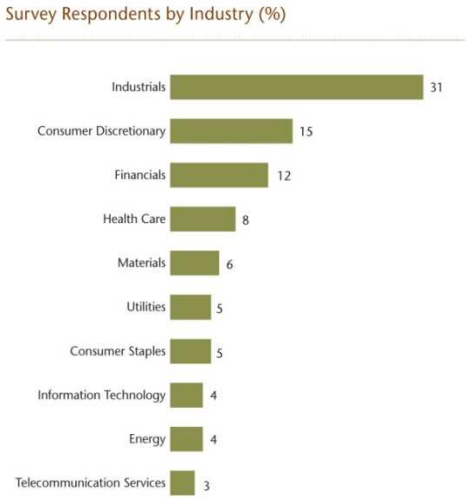
- The Global Enterprise Risk Management Survey 2010 was conducted in the third quarter of 2009 as a follow up to Aon's 2007 Enterprise Risk Management Survey.
- Assess the extent to which ERM has been successfully implemented across organizations globally.
- Determine the effect ERM has had on harmonizing organizational needs, culture and stakeholder requirements.
- Identify how ERM is being used proactively to balance risk, opportunity and value.

Methodology & Respondent Profile

- Results capture the perspectives of more than 200 responses from principal risk professionals (CRO's, CFO's, risk managers, treasurers, and others) from leading organizations around the world, representing a broad range of regions, revenues, industries & ERM maturity levels.
- Aon's five-stage ERM Maturity Model was used to help organizations benchmark their progress in driving value through ERM.







ERM Maturity Model

Figure 47

Current Stage of Development of Organization's ERM Strategy and Framework

Scale:			
1.	Initial/ Lacking	Component and associated activities are very limited in scope and may be implemented on an ad-hoc basis	11%
2.	Basic	Limited capabilities to identify, assess, manage and monitor risks	22%
3.	Defined	Sufficient capabilities to identify, measure, manage, report and monitor major risks; policies and techniques are defined and utilized (perhaps independently) across the organization	39%
4.	Operational	Consistent ability to identify, measure, manage, report and monitor risks; consistent application of policies and techniques across the organization	16%
5.	Advanced	Well-developed ability to identify, measure, manage and monitor risks across the organization; process is dynamic and able to adapt to changing risks and varying business cycles; explicit consideration of risk and risk management	7%

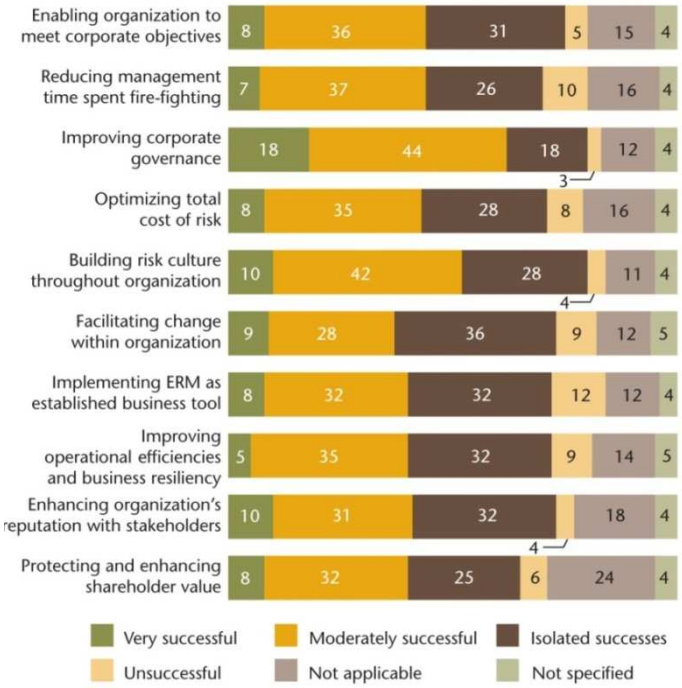
Prime Drivers of ERM

- The prime drivers for ERM implementation include improved performance, enhanced risk governance and the integration of known risk management best practices.

Prime Drivers of ERM Implementation

Corporate governance / information transparency	65%
Best practice	53%
Improved performance and decision making	49%
Regulatory pressure	23%
CEO impetus	19%
Rating agency / financial institution requirements	16%
Peer / external stakeholder pressure	9%
Other	4%
Not specified	2%

Success ERM Program has had in (%)



ERM Implementation of Barriers

- ERM journey is organic in nature and unique for each organization; it cannot be completed with a cookie-cutter approach.
- The objective is to have ERM rooted in an organization's individual culture, management processes and strategic vision, leading to enhanced risk-based decision making.
- Advanced practitioners have honed this capability and are better positioned to capitalize on emerging opportunities and extract tangible benefits from its ERM activities.

ERM Implementation Barriers

Not specified	6%
Lack of tangible benefits	40%
Lack of senior management sponsorship	31%
Lack of access to key people	12%
Lack of capital to invest in risk management	24%
Lack of skills / capability to embed ERM business	34%
Lack of clear implementation plan	28%
Failure to clearly communicate business case for change	27%
Unclear ownership / responsibility for implementation	30%
Other	7%

AON

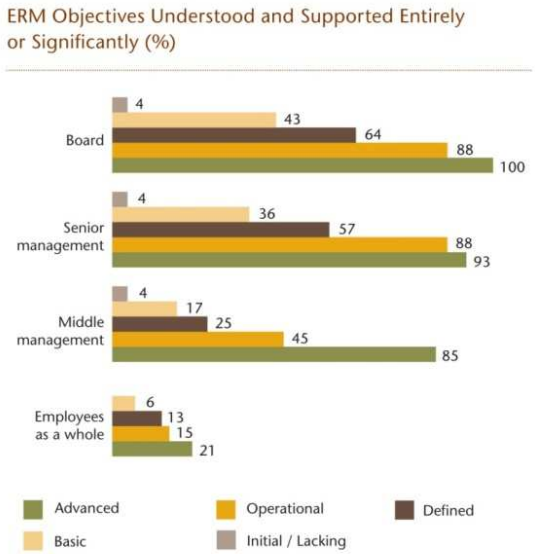
Survey Highlights

- What did we Learn about the Board and C Level roles?
- There are 10 Hallmarks of an advanced ERM Program:

1. Board Understanding and Commitment to Risk Management
2. Risk Management Stewardship
3. Risk Communication
4. Risk Culture: Engagement and Accountability
5. Risk Identification
6. Risk Management Strategy Development
7. Risk Information and Decision Making Processes
8. Risk Information and Human Capital Processes
9. Risk Analysis and Quantification
10. Risk Management Focus and Strategy

ERM C Level Hallmark No. 1
Board-Level Commitment

- enhance shareholder value. Board-level commitment to ERM as a critical framework for successful decision making and for driving value.
- Advanced ERM programs report strong board buy-in of their risk management efforts and are more likely to use risk-based information for board-level functions like strategic planning or mergers and acquisitions, and to use risk management to protect and



- **Aon's Advice:**
  - **Establish Risk Tolerance Definition and Metrics (C Level recommendation).**
  - **Include ERM in the formal corporate governance framework as a documented practice, with clear lines of responsibility and authority at board and management levels.**

ERM C Level Hallmark No. 2
Executive Stewardship

- A dedicated risk executive in a senior level position who drives and facilitates the ERM process.
- A successful “de facto” CRO:
  - has the support of the board
  - understands the strategic direction of the organization
  - has a broad view of the organization’s risks &opportunities can translate ERM into a meaningful context at every level of the organization

- **Aon’s Advice:**
  - **Risk function should report directly to the board.**
  - **Appoint an executive-level leader responsible for driving ERM strategy and implementation; someone with a detailed understanding of the business and the ability to leverage risk information from a diverse set of sources.**

ERM C Level Hallmark No. 4
Culture

- An ERM culture that encourages full engagement and accountability at all levels of the organization.
- 48% of all respondents indicated that their ERM programs have been entirely or significantly adapted to suit their individual cultures.
- Only 23% of respondents report that they reward or challenge risk taking behaviors in their performance management processes.
- .

Success Ranking in Changing / Creating a Risk Culture

Senior management setting the 'tone at the top'	74%
Clear accountabilities for risk within overall governance framework	56%
Transparency in communicating of risk information	51%
Risk information integrated into decision making	51%
Competency in analyzing / managing risk across organization	38%
Manner in which senior management responds to 'bad news'	32%
Periodic line management training in purpose / approach / methodology of ERM	30%
Sufficient resources within risk function / adequate remit to engage, challenge senior management	24%
Appropriate risk taking behaviors rewarded / challenged through performance management process	23%
Not specified	4%
Other	2%

- **Aon Advice:**
  - **Build risk thinking into corporate culture by integrating risk into existing decision making processes.**
  - **Use existing business metrics to help all levels of the organization make better risk-based decisions.**

AON

ERM C Level Hallmark No. 5
Identifying New & Emerging Risks

- Identification of new and emerging risks using internal data as well as information from external providers.
- The identification of new and emerging risks requires some degree of crystal-ball gazing and continual tweaking of what-if scenarios, and is one of the most difficult components of ERM.

Methods Used to Evaluate New and Emerging Risks

Access internal data / knowledge regarding new, emerging, developing risks	57%
Access information from external providers	54%
Develop knowledge with major project / program managers	43%
Engage stakeholders to develop information	36%
Access information from suppliers / customers	36%
Conduct cross functional "what if" analysis	35%
Develop knowledge with externally facing marketing / strategy executives	28%
No method to identify new and emerging risks	12%
Not specified	5%
Other	1%

- **Aon's Advice:**
  - **Directly link the ERM program with strategic planning to deliver the maximum value for your ERM investment.**

Conclusion

- Establish Risk Tolerance Definition and Metrics.
- Directly link the ERM program with strategic planning to deliver the maximum value for your ERM investment.
- Include ERM in the formal corporate governance framework as a documented practice, with clear lines of responsibility and authority at board and management levels.
- Demand Risk function reports directly to the board.

Global Enterprise Risk Management Survey 2010

The following ERM Maturity Self-Assessment summary is provided to help the reader quickly assess an organization's present ERM maturity level.

Assessment Criteria	Basic	Defined	Operational to Advanced
HALLMARK #1 Board-level commitment to ERM as a critical framework for successful decision making and tfor driving value	☐ The Board receives informal updates on corporate risks, typically focused on compliance and regulatory filing requirements. ☐ The management of risks is seen by the Board as being the responsibility of corporate and divisional management.	☐ The Board receives formal updates on the major corporate and business segment risks on a periodic basis. ☐ The Board questions management on the risk issues and selected risk management responses. ☐ The Board reviews the ERM framework and receives assurance that individual components are effectively implemented and managed.	☐ The Board receives formal updates on business segment, aggregated and organizational risks on an on-going basis. ☐ The Board is committed to ERM; the Board supports risk management activities with defined responsibilities including managing organizational risks in line with the risk appetite, and accounting for risk information in the evaluation of strategic plans and objectives.
HALLMARK #2 A dedicated risk executive in a senior level position who drives and facilitates the ERM process	☐ Resources are assigned to ERM on a part-time basis, without formal responsibility for developing and managing the ERM framework. ☐ ERM activities tend to be ad-hoc, reactive and uncoordinated.	☐ A formal ERM function or defined resource exists and has responsibility for developing and improving the ERM framework. Senior management supports an ERM approach but may not have defined a long term ERM strategy or vision to guide the ERM function's (or resource's) activities.	☐ ERM is sponsored by a member of the senior management team who understands the strategic direction of the organization, has a broad view of the organization's risks and opportunities, and translates this to a meaningful and strategic ERM program.
HALLMARK #3 An ERM culture that encourages full engagement and accountability at all levels of the organization	☐ Employee risk management roles and responsibilities are informally defined and not well communicated. ☐ Employees may not understand the need for or benefit of ERM.	☐ Risk management roles and responsibilities are understood at most management levels with successful ERM participation by senior management.	☐ Key areas of risk-related responsibility and accountability are clearly defined and understood by employees at all levels, enabling effective ERM.
HALLMARK #4 Engagement of all stakeholders in risk management strategy development and policy setting	☐ The bottom-up internal risk profile is developed and communicated upward in the organization to demonstrate point-in-time effectiveness of risk management practices. The information is informally referenced during strategy and policy decisions.	☐ Internal stakeholders are actively involved in the development of risk management priorities, and use key metrics to monitor and communicate the risk profile over time. ☐ Risk information is formally incorporated into strategy and policy decisions.	☐ Both internal and external stakeholders (e.g., suppliers, partners, etc.) are involved in the assessment and management of risks and the risk profile on an on-going basis. ☐ Risk information is formally incorporated into strategy and policy decisions.
HALLMARK #5 Transparency of risk communication	☐ Communication of risk information is sporadic and largely reactionary, often prompted by significant events or near misses.	☐ Efficient processes and tools to gather, refresh and access relevant risk data are established and maintained to provide needed risk information internally across the organization. ☐ Information is provided in a timely manner to relevant stakeholders.	☐ Internal and external stakeholders receive required information about organizational risks to support decisions regarding how to manage their risks. ☐ Processes are mature and efficient.

The information provided here is an extract of Aon's proprietary ERM maturity model and should not be construed as full assessment of ERM maturity, but rather as an indicator of current strengths and potential gaps in ERM practices.

Assessment Criteria	Basic	Defined	Operational to Advanced
HALLMARK #6 Integration of financial and operational risk information into decision making	☐ Little integration between ERM activities and strategic decisions at business segment and organizational levels resulting in inconsistent use of risk-based decision making.	☐ ERM risk information is consistently used in the business segments in consideration of strategic decisions (e.g., plant and manufacturing decisions, customer strategies, human resource activities, etc.), but may not be well integrated into the long-term decision making of the organization (e.g. capital allocation, market entries, new product development).	☐ Management across the organization formally considers risk information, risk tolerance and appetite, and risk mitigation strategies during decision-making activities.
HALLMARK #7 Use of sophisticated quantification methods to understand risk and demonstrate added value through risk management	☐ Qualitative analysis is used to evaluate risks in the absence of quantitative tools and capabilities.	☐ Business segments use coordinated qualitative and quantitative methods and tools to assess risk exposures and mitigation strategies of individual risks.	☐ The organization uses both qualitative and quantitative methods and tools to assess the potential impact of risk on capital, earnings, etc. ☐ The organization's risk appetite has been determined using quantitative techniques.
HALLMARK #8 Identification of new and emerging risks using internal data as well as information from external providers	☐ Business segments and the organization focus on the identification and management of day-to-day risks, often reacting to issues that materialize.	☐ Internal data and knowledge is used in the identification of internal and external risks within an established time horizon.	☐ Internal and external information (from partners, customers, competitor and industry research, other industry risk inventories, etc.) is used to identify hidden internal and external risks.
HALLMARK #9 A move from focusing on risk avoidance and mitigation to leveraging risk and risk management options to extract value	☐ Risk management focuses on problem identification and mitigation.	☐ Business segments seek opportunities to leverage risk management strengths for strategic advantage.	☐ Risk management activities focus on opportunity recognition, requiring weighing the benefit and likelihood of achieving growth against potential risk impact and cost of mitigation.
Time to develop capability*	6-12 months	1-2 years	Greater than 2 years

AON

Questions?