Risk and Insurance Management Society, Inc.®

1065 Avenue of the Americas, 13th Floor, New York, NY 10018
t (212) 286-9292 ▪ f (212) 655-5931 ▪ www.RIMS.org



August 13, 2009

Securities and Exchange Commission
Chairman Mary Shapiro
100 F Street, N.E., room 10700
Washington, D.C. 20549

RE: SEC Release NOS. 33-9052 Proxy Disclosure and Solicitation Enhancements

Dear Madame Chair:

The Securities and Exchange Commission has proposed an expansion of the disclosure requirements for public companies to include information regarding the role of the board of directors in the management of risk (SEC Release NOS. 33-9052; 34-60280; IC-28817; File S7-13). On behalf of the approximately 10,000 members of the Risk and Insurance Management Society, Inc. (RIMS), I would like to express our position that the proposed disclosures would be beneficial to shareholders and to the public and our support for the amendment of Regulation S-K to include the additional information discussed below.

RIMS believes that the current financial crisis was, to a great extent, the result of a system-wide failure to embrace appropriate enterprise risk management practices. In early 2009, RIMS issued a report entitled "2008 Financial Crisis: A Wake-up Call for Enterprise Risk Management" (see attachment) which outlines how the failure to use enterprise risk management as an integral part of organizational decision making for both risk-taking and risk-avoidance was a significant factor in the crisis and how the resulting problems might have been avoided or mitigated, if not prevented. The proposed SEC disclosure requirements represent a significant step toward correcting the deficiencies discussed in the report and RIMS believes that the additional disclosures will improve investor and shareholder understanding of the role of the board in the organization's risk management practices.

RIMS recommends that the disclosure requirements be amended as follows:

Risk and Insurance Management Society, Inc.®

1065 Avenue of the Americas, 13th Floor, New York, NY 10018
t (212) 286-9292 ▪ f (212) 655-5931 ▪ www.RIMS.org

1. The additional disclosure requirements should apply to annual and quarterly filings, proxy statements, registration statements, and information statements.
2. For registrants that meet the criteria as a Smaller Reporting Company, the following disclosures are required:
    a. The registrant shall disclose the nature of the involvement of the Board of Directors in the oversight of the risk management practices of the organization;
    b. For each director with responsibility for the risk oversight function, the registrant shall disclose the extent of that Director's specific experience, qualifications, or skills with respect to managing enterprise risk exposures comparable in breadth and complexity to the exposures expected to be raised by the registrant's operations.
3. For registrants other than a Smaller Reporting Company, the registrant shall disclose the nature of the involvement of the Board of Directors in the oversight of the risk management practices of the organization, including but not limited to the following:
    a. Whether the risk oversight function is the responsibility of the entire board or is delegated to a sub-committee of the board;
    b. If a sub-committee is used, the registrant shall disclose whether that sub-committee has responsibilities in addition to the risk oversight function and, if so, the nature of those responsibilities;
    c. If a sub-committee is used, the registrant shall disclose the percentage of sub-committee membership that is represented by independent directors;

Risk and Insurance Management Society, Inc.®

1065 Avenue of the Americas, 13th Floor, New York, NY 10018
t (212) 286-9292 ▪ f (212) 655-5931 ▪ www.RIMS.org

d. The registrant shall disclose whether the board or a sub-committee of the board establishes limitations on the total amount of and/or nature of risks to be assumed by the organization;
e. The registrant shall disclose whether the persons in management who oversee the risk management function have independent access to the Board or its designated sub-committee on issues pertaining to risk management practices;
f. The registrant shall disclose the intervals at which the status of the overall risk practices of the registrant and/or the status of significant risk management issues are reviewed, and whether such review is by the full board or its assigned sub-committee;
g. For each director with responsibility for the risk oversight function, the registrant shall disclose the extent of that Director's specific experience, qualifications, or skills with respect to managing enterprise risk exposures comparable in breadth and complexity to the exposures expected to be raised by the registrant's operations.

4. The registrant is not required to disclose specific information as to the amount or nature of the risks it has chosen to assume other than the standards already in place for Item 1A – Risk Factors.

In closing, RIMS believes that these disclosures will benefit all shareholders and investors by increasing the transparency of the registrant's risk management practices, which should lead to more widespread and effective oversight of risk.

Regards,

Joseph A. Restoule
RIMS 2009 President

Attachment

**Risk and Insurance Management Society, Inc.®**

1065 Avenue of the Americas, 13th Floor, New York, NY 10018
t (212) 286-9292 ▪ f (212) 655-5931 ▪ www.RIMS.org

RIMS Executive Report

The Risk Perspective

The

2008

Financial

Crisis

A Wake-up Call for

Enterprise Risk Management

The

2008
Financial

A Wake-up Call for

Crisis

Enterprise Risk Management

Editor

Bill Coffin

Contributors

Carol Fox, Convergys Corporation
Jeffrey Vernor, Russell Investment GroupPete Fahrenthold, Continental AirlinesRichard J. Roberts, Ensign-Bickford Industries, Inc.
Laurie Champion,Aon Global Risk Consulting
John Phelps, Blue Cross and Blue Shield of Florida, Inc.
Mary Roth, Risk and Insurance Management Society, Inc.

Art Director

Joseph Zwielich

contact: ERM@RIMS.org

3



For years, ordinary investors, encouraged by financial advisors and employers, have relied upon the securities and mutual funds held in their IRA and 401(k) accounts to retire comfortably. But all of that changed over the last 18 months, as the subprime lending crisis evolved into a full market meltdown in the second half of 2008. In short order, nearly all of Wall Street's major investment firms had either collapsed or suffered staggering losses. Even insurance giant AIG had to secure an emergency

loan from the federal government in order to avoid bankruptcy following collateral calls based on the decline of the mortgage securities underlying its credit-default-swap protection products for collateralized-debt obligations, or CDOs.1 In fact, at the end of 2008, the federal government pledged more money to bail out the financial services industry (as well as other segments of the economy) than it spent on the Louisiana Purchase, the New Deal, the Marshall Plan, the Korean War, the Race to the Moon, the Vietnam War, the Savings and Loan Crisis, Operation Iraqi Freedom, and NASA's lifetime budget combined.2

In the aftermath of such incredible market turmoil, everyday investors are left wondering how the actions taken by mid-level traders in some of the world's most prestigious financial institutions could cause not only the collapse of companies the likes of Bear Sterns and Lehman Brothers, but a wider market meltdown that has all but obliterated many personal wealth accounts. And they are not alone.

Board members and shareholders alike have expressed their outrage as companies have taken billion-dollar write downs on transactions that were calculated as remote risks in financial models created by prize-winning PhDs. Audit committees are questioning why audit risk assessments, conventional financial controls and corporate compliance activities did not reveal the extent of the potential collapse, particularly with so much emphasis given to Sarbanes-Oxley financial controls and compliance efforts.

Even former Federal Reserve Chairman Alan Greenspan has found himself explaining to congressional members that he did not expect the rapid and steep decline in market values of real estate and securities.3 After all, historical experience and conventional assumptions made no case for the kind of seismic tumult that rocked the financial markets.

In late 2007, articles in the mainstream media put the blame squarely on poor risk management practices.4 In mid-2008, as the extent of AIG's difficulties began to emerge, Maurice "Hank" Greenberg, former chairman and CEO of AIG, blamed AIG's 2008 financial meltdown on the failure of internal risk management. "Reports indicate that the risk controls my team and I put in place were weakened or eliminated after my retirement," he wrote in a statement for an October 2008 hearing by the House Committee on Oversight and Government Reform.5

In light of so many financial failures, Robert P. Hartwig, president of the Insurance Information Institute, lashed out at current enterprise risk management frameworks when he said that "the financial crisis is the result of a failure of risk management [in the banking and securities markets] on a colossal scale … We may literally have to tear up the manual of enterprise risk management and start over. How did so many major financial players miss or overlook such huge, systemic exposures?"6

In the pursuit of accountability, additional questions continue to be asked: Where were the risk managers? Why did the CFOs and Treasurers not highlight these risks? Where were the internal and external auditors? Why were executives and boards not exercising more oversight? Did the rating agencies fail to adequately understand, assess and report on risks taken by these companies? Where were the regulators? In short, who should have been protecting investors against these unintended consequences?

Was there a risk management failure?

The 2008 Financial Crisis: A Wake-up Call for Enterprise Risk Management

Some Say the Financial Crisis is a Failure of Risk Management …

1 “Behind AIG’s Fall, Risk Models Failed to Pass Real-World Test”, The Wall Street Journal, WSJ.com, October 31, 2008

2 “Bailout Payout Tops $8 Trillion,” Politico, Vol. 2, No. 104, December 16, 2008

3 “Greenspan Concedes Error on Regulation,” NYTimes.com, October 24, 2008

4 “Citigroup Acknowledges Poor Risk Management”, New York Times, October 16, 2007

5 “Pressure Builds on AIG”, Business Insurance, October 13, 2008, page 31.

6 ”Banks, Not Insurers, Need Tighter U.S. Laws Says Hartwig,” National Underwriter, 11/21/08

While it is certainly easy—and perhaps even gratifying to some—simply to lay the blame for these failures on risk management, a closer look reveals that these issues did not arise from a failure of risk management as a business discipline.

Rather, the Risk and Insurance Management Society (RIMS) contends that the financial crisis resulted from a system-wide failure to embrace appropriate enterprise risk management behaviors—or attributes—within these distressed organizations.

Additionally, there was an apparent failure to develop and reward internal risk management competencies. From the board room to the trading floor, individuals on the front line who were taking—and trading in—these risks ostensibly were rewarded for short-term profit alone.

Finally, there was a failure to use enterprise risk management to inform management’s decision making for both risk-taking and risk-avoiding decisions.

RIMS believes that several key enterprise risk

management behavioral attributes—if designed and implemented comprehensively and systemically—could have identified and mitigated, if not prevented, these losses for many of these entities.

In fact, in certain companies, enterprise risk management did make a difference. Goldman Sachs adjusted its positions in mortgage-backed securities beginning in 2006, differentiating itself from the rest of the market at a time when some might have criticized the move as excessively cautious. David Solomon, Partner and Member of the Management Committee for Goldman Sachs, attributes Goldman Sachs' risk management competencies (which are consistent with strong governance oversight, reporting, communication and culture) for its resilience in what he describes as "the perfect storm".7 Enterprise risk management can, and does, help companies perform better and avoid surprises.

Further, there is no "manual of enterprise risk management" to tear up. Risk management is a general term referring to the overall process of addressing risk, not any one particular method for mitigating risk. The term "enterprise risk management" covers risk management in the broadest possible terms, encompassing all forms of risk management activity across the entire organization.8

What's the Difference?

The terms "risk management," "enterprise risk management" and "financial risk management" are often used in ways that make it seem that the terms are interchangeable, when in fact they are not. To help distinguish between these similar-sounding concepts, some descriptions have been provided below.

"Risk Management" is a broad term for the business discipline that protects the assets and profits of an organization by reducing the potential for loss before it occurs, mitigating the impact of a loss if it occurs, and executing a swift recovery after a loss occurs. It involves a series of steps that include risk identification, the measurement and evaluation of exposures, exposure reduction or elimination, risk reporting, and risk transfer and/or financing for losses that may occur.

All organizations practice risk management in multiple forms, depending on the exposure being addressed. However, the term used to describe that process will vary based on the nature of the organization's operations. For example, both a financial institution and a non-financial institution will have risk management procedures that address the threat of damage to physical assets from hazards such as windstorm or fire. Both organizations will also have risk management processes that involve the use of hedging or derivative contracts designed to mitigate financial exposures such as interest rate or currency fluctuations. The financial institution will refer to the process of managing financial exposures as "risk management" due to the relative significance of that process to that organization. In contrast, a non-financial institution will often describe this financial exposure

mitigation process as “financial risk management” and use the term “risk management” to describe the use of insurance or similar risk transfer techniques related to the protection of physical assets. The key point is not the difference in the use of the term “risk management”. Of more importance is the fact that both these definitions indicate a significant limitation of the overall scope of the risk management process in those organizations—a limitation that is removed through the adoption of the ERM process.

Enterprise Risk Management (ERM) represents a revolutionary change in an organization’s approach to risk. ERM broadens the scope of risk management behaviors to include every significant business risk of the organization, comprehensively and systemically. It requires that all of these risks be considered in relation to each other to create a consolidated risk profile. It expands the scope of risk management practices beyond the physical and financial exposures discussed above to include issues such as long-term strategy, competitor response, human capital, and operational exposures, to name a few. In addition, ERM can potentially identify situations in which risk can be a competitive advantage instead of only a threat. ERM encompasses all aspects of an organization in managing risks and seizing opportunities related to the achievement of the organization’s objectives … not only for protection against losses, but for reducing uncertainties, thus enabling better performance against the organization’s objectives.

What
Really
Failed?

7 “Perspectives on the Current Environment and Risk Management,” The Conference Board 2008 Enterprise Risk Management Conference, David Solomon, October 22, 2008.

8 RIMS Enterprise Risk Management for Dummies®, Beaumont Vance and Joanna Makomaski, Wiley Publishing, 2007

The Risk and Insurance Management Society (RIMS) does not endorse any one enterprise risk management standard, guideline or framework.Any framework can work effectively for the company using it, if the organization demonstrates competency in seven behavioral attributes:

1. adoption of an ERM-based approach
2. ERM process management
3. risk appetite management
4. root cause discipline
5. uncovering risks
6. performance management, and
7. business resiliency and sustainability.9

There are many ways to implement an enterprise risk management program.The test in the real world is how competent the organization’s risk management practices are, and the degree to which it is instilling risk management behaviors into its culture and management’s decision-making. In short, how mature is the company’s enterprise risk management program

and how thoroughly is it practiced at all levels of the organization? So, if the present crisis is not a failure of enterprise risk management, what really failed?

There was an over-reliance on the use of financial models, with the mistaken assumption that the “risk quantifications” (used as predictions) based solely on financial modeling were both reliable and sufficient tools to justify decisions to take risk in the pursuit of profit.

The adage “All models are wrong, but some are useful”10 speaks volumes about the value of models as indicators of volatility and uncertainty–but not of certainty.A number of actuaries, financial managers and consultants regularly advocate a primarily “scientific” and quantifiable approach for enterprise risk management. Certain financial institutions seem to have replaced sound business judgment with this “scientific” approach. Even Warren Buffet, chief executive of Berkshire Hathaway Inc., is skeptical of models, telling PBS interviewer Charlie Rose,“All I can say is, beware of geeks … bearing formulas.”11

Most financial models rely on an expected distribution of losses based upon past experience. Financial institutions expect there will be certain losses, and manage these risks based on mathematical predictions of some moderate deviation from the expected norm. Since the probabilities of greater deviations are commonly believed to be insignificant (and returns often are lucrative), the tails on the financial models generally end up being ignored … and perhaps not fully understood. According to a Wall Street Journal article,AIG said in a 2006 SEC filing that its credit default swaps had never experienced high enough defaults to consider the likelihood of making a payout on its credit-default-swap protection products more than “remote, even in severe recessionary market scenarios”.12

Excessive reliance on models, combined with inadequate understanding of the assumptions underlyingthe math and lack of attention to the predicted “tail risk”, drove acceptance of risk beyond what the organizations involved could sustain in a worst-case scenario.

Even rating agencies can fall prey to the wrongfulassumptionthatremoterisksaresosmallthattheycan beexcluded from risk analysis. Media reports indicate thatin2007Citigroup’smortgage-relatedsecurities were “viewed by the rating agencies to have an extremely low probability of default (less than .01%)”.13

Geoff Riddell, chief executive of Zurich Global Corporate, explained in a study published by Zurich Financial Services Group,“The world does not follow a normal distribution and low frequency and high severity events can appear at any time.The discounting of these extremes is very dangerous.”14

Organizations that ignore the worst case scenarios regardless of low probability (the “tail risk” predicted by the models) do so at their own peril.This can be particularly disastrous if the underlying assumptions

that are embedded in financial models are accepted without question.

Mr. Riddel adds,“You have to apply common sense and ask does this scenario make sense. Quantitative tools are essential but not sufficient.”15

Just as a doctor may miss an important medical diagnosis based solely on reading a patient’s heart rate and blood pressure, financial modeling can raise important issues, but entirely miss other areas that present equal or more serious consequences.

9

RIMSRiskMaturityModelforEnterpriseRiskManagement,©2006byRiskandInsuranceManagementSociety,Inc.
10George E.P. Box,“Robustness in the strategy of scientific model building,” page 202 of Robustness in Statistics, R.L. Launer and G.N.Wilkinson, Editors.
1979 11“Behind AIG’s Fall, Risk Models Failed to Pass Real-World Test,”Wall Street Journal,WSJ.com, October 31, 2008 12Ibid.
13“The Reckoning: Citigroup Saw No Red Flags Even as It Made Bolder Bets,” Eric Dash and Julie Creswell,

nytimes.com, November 23, 2008 14“Crisis Offers Lessons on Risk Extremes,Aggregation,” Stuart Collins,Business Insurance, Dec. 11 2008 15 Ibid.

Obviously, compliance activities and controls application have a crucial role to play in an enterprise risk management context. The danger comes from the misguided belief that compliance with regulations and implementing controls based on various and sometimes disparate standards somehow equals effective enterprise risk management.

Standard and Poor’s has been quite clear in its communications that, in assessing an organization’s enterprise risk management capabilities, it is not looking for enterprise risk management to be solely about meeting compliance and/or disclosure requirements, nor is it expecting that enterprise risk management will be a replacement for internal controls.16 Simply instituting monitored compliance programs doesn’t address emerging risks, nor do such programs take into account an organization’s unique circumstances, nor the impact that risk considerations have on the key strategic and operational decisions it faces.

Controls typically are based on standards or regulatory guidance. Standards are a collection of best practices and guidelines, which are developed collaboratively. Standards, and thus controls, evolve over time based on experience. Standards development organizations recognize that existing controls may not be adequate, therefore requiring that they be expanded or modified periodically. Controls do not evolve in scope or speed to keep up with the new risks being taken. Reliance on controls is largely a post-action proposition. Consequently, controls-based metrics also lag behavior.

So, why do organizations so often intermix or confuse

risk assessments with controls gap assessments? Perhaps, organizations wrongly conclude that if they are meeting compliance requirements, they are practicing effective enterprise risk management. Some of this confusion results from auditing perspectives that concentrate on controls as the keystone of enterprise risk management. Controls traditionally have been thought to provide management with assurances that risks are being properly managed. Unless the principles of enterprise risk management are viewed as broader than a system of effective controls, any program with such a controls-based emphasis actually does not provide "… reasonable assurance to an entity's management and board of directors" that the risks of the organization indeed are being effectively identified and managed.17 Controls and metrics using historic data are not designed to be predictive of emerging or future risks. Controls are vitally important, but they are also inadequate for such assurance.

Cars have speedometers and brakes for a reason. Credit cards have spending limits. Why? Because without them, the risks taken by the driver or shopper(s) could prove to be disastrous. Similarly, organizations need to apply the "brakes" when risks have the potential of careening an organization out of control with ruinous results.

A 2006 Conference Board study found that 54% of the Fortune 100 directors it surveyed understood their company's risk tolerance.18 Since nearly half of the directors did not know, is it appropriate for shareholders to assume that either these board members were uninformed, or that management hadn't established risk tolerance levels? Given the current economic crisis, should the following board question "Do you understand management's risk tolerance level?" be supplemented with "How has that level been communicated, controlled, and monitored within the organization?" One can only speculate that if a fully understood risk tolerance level had been imposed by all financial institutions on their respective mortgage securities exposures and the marketing of collateralized debt obligations (regardless of probability metrics), the current crisis may have been mitigated to a large extent, if not prevented altogether.

It is not surprising that risk appetite management, which includes setting appropriate risk tolerance levels, was one of the three least mature competencies revealed by RIMS State of ERM Report 2008.19

There was an over-reliance on compliance and controls to protect assets, with the mistaken assumption that historic controls and monitoring a few key metrics are enough to change human behavior.

There was 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.

16 "S&P's Approach to Including ERM in Corporate Credit Ratings", Terry Pratt, Standards and Poor's, RIMS ERM

Summit November 6, 2008

17 “Enterprise Risk Management-Integrated Framework-
Executive Summary”, Committee of Sponsoring
Organizations of the Treadway Commission, September 2004

18 “CEO Challenge 2006: Top Ten Challenges,” The Conference
Board, 2006

19 RIMS State of ERM Report 2008, ©2008 by Risk and
Insurance Management Society, Inc. November 2008

Ataminimum,organizationsneedsomesortofmechanism
to “apply the brakes” once certain thresholds are about
to be exceeded. Goldman Sachs, for example, limits
its risk thresholds to levels that are expected to be
breached,“forcing conversation” and escalation.20

Recognizing that hedging does not fully transfer a risk
actually should create even more diligence in working
through—and escalating—potential worst-case
scenarios.While risk transfer certainly is a widely
accepted risk management option, presumably bundling
and transferring all of the risk potentially creates its own
problems. In particular, counterparties need to spend
considerable time understanding these more complex,
difficult risks and how they might inter-relate.When an
organization doesn’t retain some “skin in the game”,
moral hazards can be created. By way of example,
insurance underwriters recognized long ago that
effective risk management is driven when the interests
of the insured and the insurance company are “aligned”
through deductibles, retentions or coinsurance
provisions.

There was a failure to embed enterprise risk management best practices
from the top all the way down to the trading floor, with the mistaken
assumption that there is only one way to view a particular risk.

Senior leadership may sponsor the development of an
enterprise risk management program, but that is not
enough for its foundational principles to take root and
flourish. Behavior at the highest levels of the organization,
at the parent and subsidiary level reinforced through
risk-performance measurement, builds a culture of
risk-adjusted decision-making throughout an organization.
The techniques and methodology must be used
comprehensively at every level of the enterprise.

Enterprise risk management is not a panacea for all of
the uncertainties facing companies. Nor is it a guarantee
thatbadthingswillneverhappen.Afterall,organizations
cannot create and capture value without assuming some
level of risk.

Nevertheless, merely implementing a risk management
process across an enterprise clearly is not enough.RIMSState of ERM Report 2008
found that organizations
seeking better performance need to broaden and
deepen their programs to mature in the competency
drivers that support front-line risk ownership, linkage

and governance oversight.21 Oversight includes risk practitioner access to higher levels in the organization when significant risks are not being properly addressed.

Humans are conditioned to anchor beliefs based on past experience and what they know. Medical practitioners have a favorite saying for explaining misdiagnoses, “What we think are horses’ hooves actually turns out to be a zebra.”The same malady befalls risk practitioners, at times.An enlightening example can be found in a New York Times article in which Citigroup CFO Gary L. Crittenden admits misreading the credit risk of collateralized debt obligation securities.“We had a market-risk lens looking at those products, not the credit-risk lens looking at those products,” Crittenden said,“when it in fact was a credit event.”As a result, Citigroup was caught off guard by its own practices.22

20“Perspectives on the Current Environment and Risk Management”,The Conference Board 2008 Enterprise Risk Management Conference, David Solomon, October 22, 2008.

21RIMS State of ERM Report 2008, ©2008 by Risk and Insurance Management Society, Inc. November 200822“Citigroup Acknowledges Poor Risk Management,”
Eric Dash,New York Times, October 16, 2007

Even so, risk management warnings ultimately can be ignored or dismissed by management. In speaking of the failures at Fannie Mae and Freddie Mac, Rep. Henry Waxman, chairman of the House Oversight and Government Reform Committee, said “Their own risk managers raised warning after warning about the dangers of investing heavily in the subprime and alternative mortgage market. But these warnings were ignored” by the two chief executives.23 This example illustrates an enterprise risk management governance failure that prevented a direct connection between the risk management function and the persons responsible for monitoring the adherence to risk management principles, including risk tolerance limits. It is a problem we have seen in the past with failed governance oversight in companies such as Enron and Citigroup.24 In all of these cases, the persons responsible for putting on the brakes (the Board, the Risk Committee, et al.) were not getting the message directly from those sounding the alarms. With no governance structure segregating management risk oversight responsibilities from operational results, and no authorized escalation avenues, the risk management function can too easily be disregarded, despite the wisdom of its warnings—especially when it can be so neatly compartmentalized into a particular silo to be overlooked, ignored or forgotten.

The first lesson is to better understand expected and desired outcomes and to design the organization’s enterprise risk management program accordingly. Determine whether the organization is mainly concerned with the downside protection (resiliency), upside

opportunity (sustainability) or some combination of both. If emerging risks are to be cared for, what needs to be in place? Keep in mind that if the organization's focus is compliance-based, it will produce a compliance-based outcome.

Second, it is important to realize that merely implementing an enterprise risk management program is not enough. The key to successful enterprise risk management practices depends on the behavioral attributes of the organization at all levels. The organizational competencies identified as least mature from the RIMS State of ERM Report 2008, based on responses from 564 companies globally, provides an insightful view into areas for the opportunity of greatest organizational improvement.25 These least mature attributes include risk appetite and risk tolerance, root cause discipline, and performance management.

Additionally, the individual skills of those responsible for leading the risk activities within an organization provide insight into the competencies needed to drive a sustainable risk program. The graphic on this page illustrates the broad suite of skills needed for sound risk management. The enterprise risk manager will need to pay special attention to developing leadership skills, strategic thinking, ethical judgment, innovative decision-making and communication, to name a few.

What Can We Learn from the Financial Crisis?

No

Governance

Failsafe

Conceptual Skills

Planning

Organizing

Decision-making

Management Process

Ethical Judgement

Organizational Architect

Strategic Thinking

Core Competency Skills

23 "Former Fannie Mae, Freddie Mac Executives Ignored Warnings," Associated Press, December 9, 2008

24 "The Reckoning: Citigroup Saw No Red Flags Even as It Made Bolder Bets," Eric Dash and Julie Creswell,

nytimes.com, November 23, 2008

25 RIMS State of ERM Report 2008 © Risk and Insurance Management Society, Inc., November 2008

Interpersonal Skills:

Leadership

Motivator

Negotiations

Consensus Builder

Team Builder

Personal Skills:

Motivated

Innovative

Experienced

Communication

Consultative

Technical Skills

Risk Management Process

Risk Analysis

Risk Control

Risk Financing

Enterprise Risk Management

Project Management

Insurance Knowledge

Vendor Relations

ERMIS & Claims Management

Business Skills

Accounting

Economics

Finance

Legal

Compliance

Human Resources

Audit

Management

Information

Technology

Marketing

Operations

Statistics

Security

Safety

Source: RIMS Core Competency Model

8



Enterprise risk management must be part of the culture—accepted, expected and practiced at the highest levels and down through the organization—if it is to help the organization make better risk-adjusted decisions.

In RIMS State of ERM Report 2008, mature programs exhibit three foundational capabilities: front-line risk participation, linkage between risk and objectives, and governance oversight. While all three are important, the first has special significance, as it was highlighted as the one driver out of a possible 25 ("extensive involvement in ERM by front-line management at all levels") that was most highly correlated with higher credit ratings and the ability to sustain better performance.

These findings contradict the notion that effective enterprise risk management can be achieved simply through a top-down implementation. Rather, enterprise risk management is most effective when it spurs a change in how everyone in the organization thinks about, and acts upon, the risks to the organization.

RIMS believes that the 2008 financial crisis is a call to action for enterprise risk management to demonstrate its value. It requires practitioners to exhibit the personal characteristics referenced earlier—leadership, ethical decision making and a strategic point of view. But it also requires a certain degree of courage in cases where a company's culture is not yet ready to embrace ERM fully. As Chris Duncan, former Chief Risk Officer of Delta Airlines, said in a November 2008 editorial, "… for ERM to be effective, occasionally one does have to swim against the tide and run the risk of getting eaten by the sharks."26

Ultimately, when we look for a cause of the current financial crisis, it is critical to remember that organizations failed to do a number of things:

a) truly adopt an enterprise risk management culture

b) embrace and demonstrate appropriate enterprise risk management behaviors, or attributes

c) develop and reward internal risk management competencies, and

d) use enterprise risk management to inform management decision-making in both taking and avoiding risks.

Enterprise risk management—to be effective—must fundamentally change the way organizations think about risk. When enterprise risk management becomes part of the DNA of a company's culture, the warning signs of a market gone astray cannot go unseen so easily. When every employee is part of a larger risk management process, companies can be much more resilient in the face of risks. It is an important lesson to learn now, before the cycle renews itself and businesses find themselves facing the next cycle of business failures, lapses in risk management and shortcomings in governance. The cycle does not have to repeat itself as it always has in the past. Enterprise risk management is an important key to preventing it.

Enterprise risk management, when designed and implemented comprehensively and systemically, can change future outcomes. When it is practiced fully, enterprise risk management does not just help protect businesses from setbacks, it enables better overall business performance. With that in mind, and with so much economic uncertainty on the horizon, now is the perfect opportunity for organizations to use the many strengths of a solid enterprise risk management program to their advantage. Moreover, the Risk and Insurance Management Society, as a leading advocate of enterprise risk management, is uniquely positioned to help drive leadership competencies in enterprise risk management.

Conclusion

Effective
Enterprise Risk
Management

26 "Where Was ERM?" by Christopher Duncan, November 2008, IRMI.com

9

About the Risk and Insurance Management Society, Inc.

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to advancing the practice of risk management. Founded in 1950, RIMS represents some 4,000 industrial, service, nonprofit, charitable and government entities. The Society serves more than 10,500 risk management professionals around the world.

About the ERM Center of Excellence

RIMS ERM Center of Excellence is the risk professional’s source for news, tools and peer-to-peer networking on everything related to Enterprise Risk Management. Whether you are initiating an ERM program within your organization, in the implementation phase or streamlining processes, in RIMS ERM Center of Excellence you will gain access to the key information and connect with the risk practitioners that will put you on the road to ERM success.

Find more information on RIMS programs and services, to enroll in membership or access RIMS ERM Center of Excellence, visit www.RIMS.org and www.RIMS.org/ERM.

RIMS

1065 Avenue of the Americas

13th Floor

New York, NY 10018

Tel:212-286-9292

email: ERM@RIMS.org

www.RIMS.org